

日 本 国 特 許 庁
JAPAN PATENT OFFICE

J1046 U.S. PTO
09/870207
05/30/01

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日
Date of Application:

2001年 4月 2日

出 願 番 号
Application Number:

特願2001-103153

出 願 人
Applicant(s):

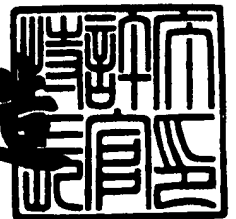
ソニー株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2001年 5月11日

特 許 庁 長 官
Commissioner,
Japan Patent Office

及 川 耕 造



【書類名】 特許願

【整理番号】 0100242111

【提出日】 平成13年 4月 2日

【あて先】 特許庁長官殿

【国際特許分類】 H04N 7/08

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

【氏名】 江▲崎▼ 正

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

【氏名】 平井 純

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

【氏名】 佐藤 英雄

【特許出願人】

【識別番号】 000002185

【氏名又は名称】 ソニー株式会社

【代表者】 出井 伸之

【代理人】

【識別番号】 100101801

【弁理士】

【氏名又は名称】 山田 英治

【選任した代理人】

【識別番号】 100093241

【弁理士】

【氏名又は名称】 宮田 正昭

【選任した代理人】

【識別番号】 100086531

【弁理士】

【氏名又は名称】 澤田 俊夫

【先の出願に基づく優先権主張】

【出願番号】 特願2000-162319

【出願日】 平成12年 5月31日

【手数料の表示】

【予納台帳番号】 062721

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9904833

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 コンテンツ・コピー管理システム及び方法、情報処理装置及び方法、サーバ、並びに、記憶媒体

【特許請求の範囲】

【請求項1】

コンテンツの外部機器へのコピーを管理するコンテンツ・コピー管理システムであって、

コピー対象となるコンテンツを読み込む手段と、

コピー対象となるコンテンツの識別情報を読み込む手段と、

各コンテンツのコピー可否情報を保管するデータベースと、

コンテンツに挿入された電子透かしを検査する電子透かし検査手段と、

コンテンツの外部機器へのコピー動作を制御するコピー制御手段と、

を具備し、

前記コピー制御手段は、コピー対象となるコンテンツの識別情報及び／又は属性情報を基に前記データベースを検索し、該当するレコードが存在する場合にはそのレコードの内容に応じてコピー動作を制御し、該当するレコードが存在しない場合には前記電子透かし検査手段による該コンテンツの検査結果に応じてコピー動作を制御することを特徴とするコンテンツ・コピー管理システム。

【請求項2】

前記コピー制御手段は、コンテンツを圧縮及び暗号化してから前記外部機器にコピーすることを特徴とする請求項1に記載のコンテンツ・コピー管理システム。

【請求項3】

前記コピー制御手段と前記データベースは安全な通信路を介して接続されていることを特徴とする請求項1に記載のコンテンツ・コピー管理システム。

【請求項4】

さらに、コピー対象となるコンテンツの属性情報を取得する手段を備え、

前記属性情報は、コンテンツの一部を切り取ったデータであることを特徴とする請求項1に記載のコンテンツ・コピー管理システム。

【請求項 5】

さらに、コピー対象となるコンテンツの属性情報を取得する手段を備え、
前記属性情報は、コンテンツの一部又は全部のハッシュ値であることを特徴とする請求項 1 に記載のコンテンツ・コピー管理システム。

【請求項 6】

さらに、コピー対象となるコンテンツの属性情報を取得する手段を備え、
前記属性情報は、コンテンツのエンベロープ値、リズムに相当する周期、スペクトルの広がり方などのコンテンツに関する特徴値又は特徴量であることを特徴とする請求項 1 に記載のコンテンツ・コピー管理システム。

【請求項 7】

コンテンツの外部機器へのコピーを管理するコンテンツ・コピー管理方法であって、

コピー対象となるコンテンツを読み込むステップと、

コピー対象となるコンテンツの識別情報を読み込むステップと、

コピー対象となるコンテンツの識別情報及び／又は属性情報を基にして各コンテンツのコピー可否情報を保管するデータベースに対して問い合わせるステップと、

該データベース中に該当するレコードが存在する場合にはそのレコードの内容に応じてコピー動作を制御するステップと、

該データベース中に該当するレコードが存在しない場合にはコンテンツ中に挿入された電子透かしの検査結果に応じてコピー動作を制御するステップと、
を具備することを特徴とするコンテンツ・コピー管理方法。

【請求項 8】

前記コピー動作を制御するステップでは、コンテンツを圧縮及び暗号化してから前記外部機器にコピーすることを特徴とする請求項 7 に記載のコンテンツ・コピー管理方法。

【請求項 9】

前記データベースへの問合せは安全な通信路を介して行われることを特徴とする請求項 7 に記載のコンテンツ・コピー管理方法。

【請求項 1 0】

さらに、コピー対象となるコンテンツの属性情報を取得するステップを備え、
前記属性情報は、コンテンツの一部又は全部を切り取ったデータであることを
特徴とする請求項 7 に記載のコンテンツ・コピー管理方法。

【請求項 1 1】

さらに、コピー対象となるコンテンツの属性情報を取得するステップを備え、
前記属性情報は、コンテンツの一部又は全部のハッシュ値であることを特徴と
する請求項 7 に記載のコンテンツ・コピー管理方法。

【請求項 1 2】

さらに、コピー対象となるコンテンツの属性情報を取得するステップを備え、
前記属性情報は、コンテンツのエンベロップ値、リズムに相当する周期、スペ
クトルの広がり方などのコンテンツに関する特徴値又は特徴量であることを特徴
とする請求項 7 に記載のコンテンツ・コピー管理方法。

【請求項 1 3】

コンテンツの外部機器へのコピー動作を実行する情報処理装置であって、
コピー対象となるコンテンツを読み込む手段と、
コピー対象となるコンテンツの識別情報を読み込む手段と、
コンテンツに挿入された電子透かしを検査する電子透かし検査手段と、
コンテンツの外部機器へのコピー動作を制御するコピー制御手段と、
を具備し、

前記コピー制御手段は、コピー対象となるコンテンツの識別情報及び／又は属
性情報を基に外部サーバに対して問合せを行い、該問合せ結果に応じて、コンテ
ンツのコピー動作を実行するか、又は、前記電子透かし検査手段による該コンテ
ンツの検査を実行して該検査結果に従ってコピー動作を制御することを特徴とす
る情報処理装置。

【請求項 1 4】

前記コピー制御手段は、コンテンツを圧縮及び暗号化してから前記外部機器に
コピーすることを特徴とする請求項 1 3 に記載の情報処理装置。

【請求項 1 5】

前記外部サーバとは安全な通信路を介して接続されていることを特徴とする請求項 13 に記載の情報処理装置。

【請求項 16】

さらに、コピー対象となるコンテンツの属性情報を取得する手段を備え、
前記属性情報は、コンテンツの一部を切り取ったデータであることを特徴とする請求項 13 に記載の情報処理装置。

【請求項 17】

さらに、コピー対象となるコンテンツの属性情報を取得する手段を備え、
前記属性情報は、コンテンツの一部又は全部のハッシュ値であることを特徴とする請求項 13 に記載の情報処理装置。

【請求項 18】

さらに、コピー対象となるコンテンツの属性情報を取得する手段を備え、
前記属性情報は、コンテンツのエンベロップ値、リズムに相当する周期、スペクトルの広がり方などのコンテンツに関する特徴値又は特徴量であることを特徴とする請求項 13 に記載の情報処理装置。

【請求項 19】

コンテンツの外部機器へのコピー動作を実行する情報処理方法であって、
コピー対象となるコンテンツを読み込むステップと、
コピー対象となるコンテンツの識別情報を読み込むステップと、
コピー対象となるコンテンツの識別情報及び／又は属性情報を基に外部サーバに対して問合せを行うステップと、

該問合せ結果に応じて、コンテンツのコピー動作を実行するか、又は、コンテンツに挿入された電子透かしの検査を実行して該検査結果に従ってコピー動作を制御するステップと、

を具備することを特徴とする情報処理方法。

【請求項 20】

前記コピー動作を制御するステップでは、コンテンツを圧縮及び暗号化してから前記外部機器にコピーすることを特徴とする請求項 19 に記載の情報処理方法。

【請求項21】

前記外部サーバへの問合せは安全な通信路を介して行うことを特徴とする請求項19に記載の情報処理方法。

【請求項22】

さらに、コピー対象となるコンテンツの属性情報を取得するステップを備え、前記属性情報は、コンテンツの一部を切り取ったデータであることを特徴とする請求項19に記載の情報処理方法。

【請求項23】

さらに、コピー対象となるコンテンツの属性情報を取得するステップを備え、前記属性情報は、コンテンツの一部又は全部のハッシュ値であることを特徴とする請求項19に記載の情報処理方法。

【請求項24】

さらに、コピー対象となるコンテンツの属性情報を取得するステップを備え、前記属性情報は、コンテンツのエンベロップ値、リズムに相当する周期、スペクトルの広がり方などのコンテンツに関する特徴値又は特徴量であることを特徴とする請求項19に記載の情報処理方法。

【請求項25】

各コンテンツに関するコピー可否情報を管理するサーバであって、コンテンツの識別情報及び／又は属性情報を基に検索可能なデータベースと、コンテンツのコピー可否に関する問合せを受信する受信手段と、該問合せに応答して前記データベースを検索する検索手段と、前記データベースの検索結果を問い合わせ元に送信する送信手段と、を具備することを特徴とするサーバ。

【請求項26】

問合せ元とは安全な通信路を介して接続されることを特徴とする請求項25に記載のサーバ。

【請求項27】

前記属性情報は、コンテンツの一部を切り取ったデータであることを特徴とする請求項25に記載のサーバ。

【請求項 2 8】

前記属性情報は、コンテンツの一部又は全部のハッシュ値であることを特徴とする請求項 2 5 に記載のサーバ。

【請求項 2 9】

前記属性情報は、コンテンツのエンベロップ値、リズムに相当する周期、スペクトルの広がり方などのコンテンツに関する特徴値又は特徴量であることを特徴とする請求項 2 5 に記載のサーバ。

【請求項 3 0】

コンテンツの外部機器へのコピーを管理する処理をコンピュータ・システム上で実行するためのコンピュータ・ソフトウェアをコンピュータ可読形式で物理的に格納したソフトウェア記憶媒体であって、前記コンピュータ・ソフトウェアは

コピー対象となるコンテンツを読み込むステップと、

コピー対象となるコンテンツの識別情報を読み込むステップと、

コピー対象となるコンテンツの属性情報を取得するステップと、

コピー対象となるコンテンツの識別情報及び／又は属性情報を基にして各コンテンツのコピー可否情報を保管するデータベースに対して問い合わせるステップと、

該データベース中に該当するレコードが存在する場合にはそのレコードの内容に応じてコピー動作を制御するステップと、

該データベース中に該当するレコードが存在しない場合にはコンテンツ中に挿入された電子透かしの検査結果に応じてコピー動作を制御するステップと、
を具備することを特徴とするソフトウェア記憶媒体。

【請求項 3 1】

前記属性情報は、コンテンツの一部又は全部を切り取ったデータであることを特徴とする請求項 3 0 に記載のソフトウェア記憶媒体。

【請求項 3 2】

前記属性情報は、コンテンツの一部又は全部のハッシュ値であることを特徴とする請求項 3 0 に記載のソフトウェア記憶媒体。

【請求項 3 3】

前記属性情報は、コンテンツのエンベロープ値、リズムに相当する周期、スペクトルの広がり方などのコンテンツに関する特徴値又は特徴量であることを特徴とする請求項 3 0 に記載のソフトウェア記憶媒体。

【請求項 3 4】

コンテンツの外部機器へのコピーを実行する処理をコンピュータ・システム上で実行するためのコンピュータ・ソフトウェアをコンピュータ可読形式で物理的に格納したソフトウェア記憶媒体であって、前記コンピュータ・ソフトウェアは

コピー対象となるコンテンツを読み込むステップと、
 コピー対象となるコンテンツの識別情報を読み込むステップと、
 コピー対象となるコンテンツの属性情報を取得するステップと、
 コピー対象となるコンテンツの識別情報及び／又は属性情報を基に外部サーバに対して問合せを行うステップと、
 該問合せ結果に応じて、コンテンツのコピー動作を実行するか、又は、コンテンツに挿入された電子透かしの検査を実行して該検査結果に従ってコピー動作を制御するステップと、
 を具備することを特徴とするソフトウェア記憶媒体。

【請求項 3 5】

前記属性情報は、コンテンツの一部又は全部を切り取ったデータであることを特徴とする請求項 3 4 に記載のソフトウェア記憶媒体。

【請求項 3 6】

前記属性情報は、コンテンツの一部又は全部のハッシュ値であることを特徴とする請求項 3 4 に記載のソフトウェア記憶媒体。

【請求項 3 7】

前記属性情報は、コンテンツのエンベロープ値、リズムに相当する周期、スペクトルの広がり方などのコンテンツに関する特徴値又は特徴量であることを特徴とする請求項 3 4 に記載のソフトウェア記憶媒体。

【請求項 3 8】

コンテンツの外部機器へのコピーを管理するコンテンツ・コピー管理システムであって、

コピー対象となるコンテンツを読み込む手段と、

コピー対象となるコンテンツの識別情報を読み込む手段と、

各コンテンツのコピー可否情報を保管するデータベースと、

コンテンツに挿入された電子透かしを検査する電子透かし検査手段と、

コンテンツを直交変換する直交変換手段と、

直交変換後のコンテンツを量子化及びハフマン符号化する符号化圧縮手段と、

前記符号化圧縮されたコンテンツを暗号化する暗号化手段と、

コンテンツの外部機器への該暗号化コンテンツのコピー動作を制御するコピー制御手段と、

を具備し、

前記コピー制御手段は、コピー対象となるコンテンツの識別情報とコンテンツの直交変換値又はそのハッシュ値を基に前記データベースを検索し、該当するレコードが存在する場合にはそのレコードの内容に応じて該暗号化コンテンツのコピー動作を制御し、該当するレコードが存在しない場合には前記電子透かし検査手段による該コンテンツの検査結果に応じて該暗号化コンテンツのコピー動作を制御することを特徴とするコンテンツ・コピー管理システム。

【請求項 39】

コンテンツの外部機器へのコピーを管理するコンテンツ・コピー管理方法であって、

コピー対象となるコンテンツを読み込むステップと、

コピー対象となるコンテンツの識別情報を読み込むステップと、

コンテンツを直交変換する直交変換ステップと、

直交変換後のコンテンツを量子化及びハフマン符号化する符号化圧縮ステップと、

前記符号化圧縮されたコンテンツを暗号化する暗号化ステップと、

コピー対象となるコンテンツの識別情報とコンテンツの直交変換値又はそのハッシュ値を基にして各コンテンツのコピー可否情報を保管するデータベースに対

して問い合わせるステップと、

該データベース中に該当するレコードが存在する場合にはそのレコードの内容に応じて該暗号化コンテンツのコピー動作を制御するステップと、

該データベース中に該当するレコードが存在しない場合にはコンテンツ中に挿入された電子透かしの検査結果に応じて該暗号化コンテンツのコピー動作を制御するステップと、

を具備することを特徴とするコンテンツ・コピー管理方法。

【請求項 4 0】

コンテンツの外部機器へのコピー動作を実行する情報処理装置であって、

コピー対象となるコンテンツを読み込む手段と、

コピー対象となるコンテンツの識別情報を読み込む手段と、

コンテンツに挿入された電子透かしを検査する電子透かし検査手段と、

コンテンツを直交変換する直交変換手段と、

直交変換後のコンテンツを量子化及びハフマン符号化する符号化圧縮手段と、

前記符号化圧縮されたコンテンツを暗号化する暗号化手段と、

コンテンツの外部機器への該暗号化コンテンツのコピー動作を制御するコピー制御手段と、

を具備し、

前記コピー制御手段は、コピー対象となるコンテンツの識別情報とコンテンツの直交変換値又はそのハッシュ値を基に外部サーバに問合せを行い、該問合せ結果に応じて、該暗号化コンテンツのコピー動作を実行するか、又は、前記電子透かし検査手段による該コンテンツの検査結果に応じて該暗号化コンテンツのコピー動作を制御することを特徴とする情報処理装置。

【請求項 4 1】

コンテンツの外部機器へのコピー動作を実行する情報処理方法であって、

コピー対象となるコンテンツを読み込むステップと、

コピー対象となるコンテンツの識別情報を読み込むステップと、

コンテンツを直交変換する直交変換ステップと、

直交変換後のコンテンツを量子化及びハフマン符号化する符号化圧縮ステップ

と、

前記符号化圧縮されたコンテンツを暗号化する暗号化ステップと、

コピー対象となるコンテンツの識別情報とコンテンツの直交変換値又はそのハッシュ値を基に外部サーバに問合せを行うステップと、

該問合せ結果に応じて、該暗号化コンテンツのコピー動作を実行するか、又は、コンテンツ中に挿入された電子透かしの検査結果に応じて該暗号化コンテンツのコピー動作を制御するステップと、

を具備することを特徴とする情報処理方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、画像や音楽などのコンテンツ中に、ほとんど目に見えない又は耳に聞こえない形で情報を埋め込む電子透かし技術に係り、特に、映像や音楽、放送番組などの各種コンテンツに埋め込まれた電子透かしを検査する電子透かし検査技術に関する。

【0002】

更に詳しくは、本発明は、コンテンツに埋め込まれた電子透かしを検査した結果に従ってコンテンツの複製の可否を判断する電子透かし検査技術に係り、特に、計算負荷の高い電子透かし検査処理を代行して行う電子透かし検査技術に関する。

【0003】

【従来の技術】

著作権とは、著作物を利用し得る相対的な排他的独占権であり、いわゆる無体財産権の1つに含まれる。ここで言う「著作物」とは、思想又は感情を創作的に表現したものであって、文芸、学術、美術又は音楽の範囲に属するものを指す。著作権は、各国の著作権法や、ベルヌ条約や万国著作権条約などの国際的な条約で保護されている。例えば、デジタル化されたテキストやコンピュータ・プログラム、デジタル化された音楽コンテンツ、映像コンテンツ、番組の放送コンテンツなど各種のメディアも著作物であり、著作権法制下で適正に保護を受けるべき

である。

【0004】

著作権者自身においてのみ著作物の利用が行われるのはごく稀であり、他人が著作権を利用することに対して著作権者が一定の対価を得て許諾するというのが一般的である。したがって、著作権の保護を担保するためには、他人が勝手に（許可なく）著作物を複製するなどの著作物の不正使用を防止する必要がある。

【0005】

著作権保護の歴史は15世紀中ごろの印刷技術の発明に由来すると言われているが、昨今における電気・電子技術の飛躍的な進歩により著作物の複製が技術的に容易となってきているので、著作権をめぐる情勢も時々刻々と変貌してきている。

【0006】

デジタル形式のデータやコンテンツの複製や改竄は極めて容易であり、著作権侵害の危険に無防備にさらされているとさえ言える。したがって、著作権法やその他の法規制を強化するだけでは不十分であり、情報技術の観点からも著作物の正当な利用を支援し若しくは不正利用を排除して、著作権の保護を拡充する必要があると思料される。

【0007】

デジタル・コンテンツの世界において、不正コピーに対抗するための1つの手段として「電子透かし」（Digital Watermarking 又はData Hidingとも言う）と呼ばれる技術を挙げることができる。電子透かしとは、画像や音楽などのコンテンツ中に、ほとんど目に見えない又は耳に聞こえない形で情報を埋め込むことを意味する（例えば、「電子透かしを支えるデータ・ハイディング技術（上・下）」（日経エレクトロニクス1997年2月24日号並びに同年3月10日号）を参照のこと）。

【0008】

電子透かしは、埋め込み先であるホスト信号の統計的性質を利用して、ホスト信号の一部に元の情報とは異なる情報を挿入することで実現される。例えば、著作権情報を電子透かしにより埋め込むことで、後にコンテンツを採取したときに

、透かしすなわち著作権情報を浮き上がらせて、データの流通経路や使用権の有無を検査したり、コピー制御情報を検証することができる。

【0009】

例えば、デジタル音楽の著作権保護を目的として、1998年に米国大手レコード会社などが中心となってSDMI (Secure Digital Music Interactive) なるフォーラムが設立された。SDMIでは、ポータブル音楽プレーヤで著作権を保護する仕組みとして“Screening”という機能が規定されている。Screeningとは、ポータブル・デバイス(PD)のメモリ・レコーダ上にコピーしてよいコンテンツか否かを検査する仕組みであり、電子透かしを利用することが既に合意されている。例えば、不正に配信されたコンテンツや、既に1回(若しくは許容回数だけ)コピーされたコンテンツからはもはやコピーできないように、電子透かしによってScreeningをかけることができる。

【0010】

図1には、SDMIで想定しているScreening処理を行う機能ブロック図を模式的に示している。同図に示すように、CDやMDのような記録メディアから読み取った音楽コンテンツ、あるいは通信媒体経由で受信した音楽コンテンツに対してまずScreeningにかけて(すなわち電子透かしを検査して)、コピー可能か否かをチェックした後、LCM (Licensed SDMI Compliant Module) という仕組みで圧縮暗号化してから、携帯型機器(PD)上にコピーする。ここで言う、携帯型機器とは、圧縮暗号化されたデータ・コンテンツを伸張及び解読処理してコンテンツ再生する機能を持つポータブル・デバイス/プレーヤである。

【0011】

図1に示すようなScreening処理システムは、例えば、パーソナル・コンピュータのような計算機システム上で実装され、携帯型機器との間は、例えば、i-link, USB (Universal Serial Bus) のような汎用バス・ケーブル、あるいはIrDA (Infrared Data Association) やBluetoothのような近接無線データ通信によって接続されている。

【0012】

電子透かしは、音楽コンテンツ中に、耳に聞こえない程度に付加的なデータを挿入する技術であり、通常、約15秒間に12ビット程度のデータを挿入することができる。

【0013】

ところで、電子透かしを検出するのには計算負荷が重く、時間がかかるという問題がある。例えば、音楽コンテンツ全体にわたって電子透かしを検査しようとすると、実演奏時間の1/2～1/3程度の計算時間を要してしまう。

【0014】

ここで、上記のScreening処理をパーソナル・コンピュータ上で実装して、CDから音楽コンテンツを携帯型機器上にコピーする場合について考察してみると、以下のような過程から構成される。すなわち、

【0015】

(1) CDからデータを読み出して、ハード・ディスク上にWAV形式（あるいは他のフォーマットでも可）ファイルとしてコピーする。

(2) WAVファイルを検査して、音楽データ全体にわたって電子透かしを検出する。

(3) 電子透かしから”No More Copy”なるコピー禁止情報が検出されたなら、その時点で音楽コンテンツコピー処理を停止する。他方、かかるコピー禁止情報が検出されない場合には、楽曲の最後まで検出処理を継続して、最終的に検出されなかったら次のステップ(4)に進む。

(4) WAVファイルを例えばATRAC3 (Adaptive Transform Acoustic Coding 3)などで帯域圧縮する。

(5) 帯域圧縮されたデータを暗号化して、ハード・ディスク上に一旦コピーする。

(6) ハード・ディスク上の圧縮暗号化ファイルを携帯型機器に転送する。

【0016】

ここで、電子透かしが挿入されていない従来のCDからのコピーを試みた場合には、本来はScreeningにかけること自体意味がないにも拘わらず、上記のステップ(3)において、最終的にすべてのデータをチェックすることにな

ってしまい、検出時間に余分な時間がかかってしまう。例えば、ユーザが出かける前などに、急いでCDから携帯型機器に好きな音楽をコピーしたいような場合には、利便性を大いに損なう結果となる。

【0017】

【発明が解決しようとする課題】

本発明の目的は、コンテンツに埋め込まれた電子透かしを検査することができる、優れた電子透かし検査技術を提供することにある。

【0018】

本発明の更なる目的は、コンテンツに埋め込まれた電子透かしを検査した結果に従ってコンテンツの複製の可否を判断することができる、優れた電子透かし検査技術を提供することにある。

【0019】

本発明の更なる目的は、計算負荷の高い電子透かし検査処理を代行して、コンテンツの複製の可否を判断し、コピー操作全体に要する時間を短縮することができる、優れた電子透かし検査技術を提供することにある。

【0020】

【課題を解決するための手段】

本発明は、上記課題を参酌してなされたものであり、その第1の側面は、コンテンツの外部機器へのコピーを管理するコンテンツ・コピー管理システムであって、

コピー対象となるコンテンツを読み込む手段と、

コピー対象となるコンテンツの識別情報を読み込む手段と、

各コンテンツのコピー可否情報を保管するデータベースと、

コンテンツに挿入された電子透かしを検査する電子透かし検査手段と、

コンテンツの外部機器へのコピー動作を制御するコピー制御手段と、

を具備し、

前記コピー制御手段は、コピー対象となるコンテンツの識別情報及び／又は属性情報を基に前記データベースを検索し、該当するレコードが存在する場合にはそのレコードの内容に応じてコピー動作を制御し、該当するレコードが存在しな

い場合には前記電子透かし検査手段による該コンテンツの検査結果に応じてコピー動作を制御することを特徴とするコンテンツ・コピー管理システムである。

【 0 0 2 1 】

ここで、前記コピー制御手段は、コンテンツを圧縮及び暗号化してから前記外部機器にコピーするようにしてもよい。

【 0 0 2 2 】

また、前記コピー制御手段と前記データベースは安全な通信路を介して接続されていることが好ましい。安全な通信路は、例えば、電子認証や鍵交換の手続きを経て確立することができる。

【 0 0 2 3 】

また、本発明の第 1 の側面に係るコンテンツ・コピー管理システムは、さらに、コピー対象となるコンテンツの属性情報を取得する手段を備えていてもよい。

【 0 0 2 4 】

このような場合、前記属性情報は、コンテンツの一部を切り取ったデータであってもよい。あるいは、前記属性情報は、コンテンツの一部又は全部のハッシュ値であってもよい。前記属性情報は、コンテンツのエンベロップ値、リズムに相当する周期、スペクトルの広がり方などのコンテンツに関する特徴値又は特徴量であってもよい。

【 0 0 2 5 】

また、本発明の第 2 の側面は、コンテンツの外部機器へのコピーを管理するコンテンツ・コピー管理方法であって、

コピー対象となるコンテンツを読み込むステップと、

コピー対象となるコンテンツの識別情報を読み込むステップと、

コピー対象となるコンテンツの識別情報及び／又は属性情報を基にして各コンテンツのコピー可否情報を保管するデータベースに対して問い合わせるステップと、

該データベース中に該当するレコードが存在する場合にはそのレコードの内容に応じてコピー動作を制御するステップと、

該データベース中に該当するレコードが存在しない場合にはコンテンツ中に挿

入された電子透かしの検査結果に応じてコピー動作を制御するステップと、
を具備することを特徴とするコンテンツ・コピー管理方法である。

【 0 0 2 6 】

前記コピー動作を制御するステップでは、コンテンツを圧縮及び暗号化してから前記外部機器にコピーするようにしてもよい。

【 0 0 2 7 】

また、前記データベースへの問合せは安全な通信路を介して行われることが好ましい。安全な通信路は、例えば、電子認証や鍵交換の手続きを経て確立することができる。

【 0 0 2 8 】

また、本発明の第 2 の側面に係るコンテンツ・コピー管理方法は、さらに、コピー対象となるコンテンツの属性情報を取得するステップを備えていてもよい。このような場合、前記属性情報は、コンテンツの一部を切り取ったデータであってもよい。あるいは、前記属性情報は、コンテンツの一部又は全部のハッシュ値であってもよい。前記属性情報は、コンテンツのエンベロップ値、リズムに相当する周期、スペクトルの広がり方などのコンテンツに関する特徴値又は特徴量であってもよい。

【 0 0 2 9 】

また、本発明の第 3 の側面は、コンテンツの外部機器へのコピー動作を実行する情報処理装置であって、

コピー対象となるコンテンツを読み込む手段と、

コピー対象となるコンテンツの識別情報を読み込む手段と、

コンテンツに挿入された電子透かしを検査する電子透かし検査手段と、

コンテンツの外部機器へのコピー動作を制御するコピー制御手段と、

を具備し、

前記コピー制御手段は、コピー対象となるコンテンツの識別情報及び／又は属性情報を基に外部サーバに対して問合せを行い、該問合せ結果に応じて、コンテンツのコピー動作を実行するか、又は、前記電子透かし検査手段による該コンテンツの検査を実行して該検査結果に従ってコピー動作を制御することを特徴とす

る情報処理装置である。

【0030】

前記コピー制御手段は、コンテンツを圧縮及び暗号化してから前記外部機器にコピーするようにしてもよい。

【0031】

また、前記外部サーバとは安全な通信路を介して接続されていることが好ましい。安全な通信路は、例えば、電子認証や鍵交換の手続きを経て確立することができる。

【0032】

また、本発明の第3の側面に係る情報処理装置は、さらに、コピー対象となるコンテンツの属性情報を取得する手段を備えていてもよい。このような場合、前記属性情報は、コンテンツの一部を切り取ったデータであってもよい。あるいは、前記属性情報は、コンテンツの一部又は全部のハッシュ値であってもよい。前記属性情報は、コンテンツのエンベロップ値、リズムに相当する周期、スペクトルの広がり方などのコンテンツに関する特徴値又は特徴量であってもよい。

【0033】

また、本発明の第4の側面は、コンテンツの外部機器へのコピー動作を実行する情報処理方法であって、

コピー対象となるコンテンツを読み込むステップと、

コピー対象となるコンテンツの識別情報を読み込むステップと、

コピー対象となるコンテンツの識別情報及び／又は属性情報を基に外部サーバに対して問合せを行うステップと、

該問合せ結果に応じて、コンテンツのコピー動作を実行するか、又は、コンテンツに挿入された電子透かしの検査を実行して該検査結果に従ってコピー動作を制御するステップと、

を具備することを特徴とする情報処理方法である。

【0034】

前記コピー動作を制御するステップでは、コンテンツを圧縮及び暗号化してから前記外部機器にコピーするようにしてもよい。

【 0 0 3 5 】

また、前記外部サーバへの問合せは安全な通信路を介して行うことが好ましい。安全な通信路は、例えば、電子認証や鍵交換の手続きを経て確立することができる。

【 0 0 3 6 】

また、本発明の第4の側面に係る情報処理方法は、さらに、コピー対象となるコンテンツの属性情報を取得するステップを備えていてもよい。このような場合、前記属性情報は、コンテンツの一部を切り取ったデータであってもよい。あるいは、前記属性情報は、コンテンツの一部又は全部のハッシュ値であってもよい。前記属性情報は、コンテンツのエンベロップ値、リズムに相当する周期、スペクトルの広がり方などのコンテンツに関する特徴値又は特徴量であってもよい。

【 0 0 3 7 】

また、本発明の第5の側面は、各コンテンツに関するコピー可否情報を管理するサーバであって、

コンテンツの識別情報及び／又は属性情報を基に検索可能なデータベースと、

コンテンツのコピー可否に関する問合せを受信する受信手段と、

該問合せに応答して前記データベースを検索する検索手段と、

前記データベースの検索結果を問い合わせ元へ送信する送信手段と、

を具備することを特徴とするサーバである。

【 0 0 3 8 】

本発明の第5の側面に係るサーバは、問合せ元とは安全な通信路を介して接続されていることが好ましい。安全な通信路は、例えば、電子認証や鍵交換の手続きを経て確立することができる。

【 0 0 3 9 】

また、前記属性情報は、コンテンツの一部を切り取ったデータであってもよい。あるいは、前記属性情報は、コンテンツの一部又は全部のハッシュ値であってもよい。前記属性情報は、コンテンツのエンベロップ値、リズムに相当する周期、スペクトルの広がり方などのコンテンツに関する特徴値又は特徴量であってもよい。

【 0 0 4 0 】

また、本発明の第 6 の側面は、コンテンツの外部機器へのコピーを管理する処理をコンピュータ・システム上で実行するためのコンピュータ・ソフトウェアをコンピュータ可読形式で物理的に格納したソフトウェア記憶媒体であって、前記コンピュータ・ソフトウェアは、

コピー対象となるコンテンツを読み込むステップと、

コピー対象となるコンテンツの識別情報を読み込むステップと、

コピー対象となるコンテンツの属性情報を取得するステップと、

コピー対象となるコンテンツの識別情報及び／又は属性情報を基にして各コンテンツのコピー可否情報を保管するデータベースに対して問い合わせるステップと、

該データベース中に該当するレコードが存在する場合にはそのレコードの内容に応じてコピー動作を制御するステップと、

該データベース中に該当するレコードが存在しない場合にはコンテンツ中に挿入された電子透かしの検査結果に応じてコピー動作を制御するステップと、
を具備することを特徴とするソフトウェア記憶媒体である。

【 0 0 4 1 】

また、本発明の第 7 の側面は、コンテンツの外部機器へのコピーを実行する処理をコンピュータ・システム上で実行するためのコンピュータ・ソフトウェアをコンピュータ可読形式で物理的に格納したソフトウェア記憶媒体であって、前記コンピュータ・ソフトウェアは、

コピー対象となるコンテンツを読み込むステップと、

コピー対象となるコンテンツの識別情報を読み込むステップと、

コピー対象となるコンテンツの属性情報を取得するステップと、

コピー対象となるコンテンツの識別情報及び／又は属性情報を基に外部サーバに対して問合せを行うステップと、

該問合せ結果に応じて、コンテンツのコピー動作を実行するか、又は、コンテンツに挿入された電子透かしの検査を実行して該検査結果に従ってコピー動作を制御するステップと、

を具備することを特徴とするソフトウェア記憶媒体である。

【0042】

本発明の第6及び第7の各側面に係るソフトウェア記憶媒体は、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ・ソフトウェアをコンピュータ可読な形式で提供する媒体である。このような媒体は、例えば、CD (Compact Disc) やFD (Floppy Disk)、MO (Magnetooptical disc) などの着脱自在で可搬性の記憶媒体である。あるいは、ネットワーク（ネットワークは無線、有線の区別を問わない）などの伝送媒体などを經由してコンピュータ・ソフトウェアを特定のコンピュータ・システムに提供することも技術的に可能である。

【0043】

このようなソフトウェア記憶媒体は、コンピュータ・システム上で所定のコンピュータ・ソフトウェアの機能を実現するための、コンピュータ・ソフトウェアと記憶媒体との構造上又は機能上の協働的關係を定義したものである。換言すれば、本発明の第6及び第7の側面に係るソフトウェア記憶媒体を介して所定のコンピュータ・ソフトウェアをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働的作用が発揮され、本発明の第1、第2、並びに、第3、第4の各側面に係るコンテンツ・コピー管理システム及び方法、並びに、情報処理装置及び方法と同様の作用効果を得ることができる。

【0044】

また、本発明の第8の側面は、コンテンツの外部機器へのコピーを管理するコンテンツ・コピー管理システムであって、

コピー対象となるコンテンツを読み込む手段と、

コピー対象となるコンテンツの識別情報を読み込む手段と、

各コンテンツのコピー可否情報を保管するデータベースと、

コンテンツに挿入された電子透かしを検査する電子透かし検査手段と、

コンテンツを直交変換する直交変換手段と、

直交変換後のコンテンツを量子化及びハフマン符号化する符号化圧縮手段と、

前記符号化圧縮されたコンテンツを暗号化する暗号化手段と、

コンテンツの外部機器への該暗号化コンテンツのコピー動作を制御するコピー制御手段と、

を具備し、

前記コピー制御手段は、コピー対象となるコンテンツの識別情報とコンテンツの直交変換値又はそのハッシュ値を基に前記データベースを検索し、該当するレコードが存在する場合にはそのレコードの内容に応じて該暗号化コンテンツのコピー動作を制御し、該当するレコードが存在しない場合には前記電子透かし検査手段による該コンテンツの検査結果に応じて該暗号化コンテンツのコピー動作を制御することを特徴とするコンテンツ・コピー管理システムである。ここで言う

「直交変換」には、例えばmDCT（変形離散コサイン変換）や、DCT（離散コサイン変換）、wavelet（"wavelet"は米サマス・テクノロジー社が開発した波形分析技術）などが含まれる（以下、同様）。

【0045】

また、本発明の第9の側面は、コンテンツの外部機器へのコピーを管理するコンテンツ・コピー管理方法であって、

コピー対象となるコンテンツを読み込むステップと、

コピー対象となるコンテンツの識別情報を読み込むステップと、

コンテンツを直交変換する直交変換ステップと、

直交変換後のコンテンツを量子化及びハフマン符号化する符号化圧縮ステップと、

前記符号化圧縮されたコンテンツを暗号化する暗号化ステップと、

コピー対象となるコンテンツの識別情報とコンテンツの直交変換値又はそのハッシュ値を基にして各コンテンツのコピー可否情報を保管するデータベースに対して問い合わせるステップと、

該データベース中に該当するレコードが存在する場合にはそのレコードの内容に応じて該暗号化コンテンツのコピー動作を制御するステップと、

該データベース中に該当するレコードが存在しない場合にはコンテンツ中に挿入された電子透かしの検査結果に応じて該暗号化コンテンツのコピー動作を制御するステップと、

を具備することを特徴とするコンテンツ・コピー管理方法である。

【 0 0 4 6 】

また、本発明の第 1 0 の側面は、コンテンツの外部機器へのコピー動作を実行する情報処理装置であって、

コピー対象となるコンテンツを読み込む手段と、

コピー対象となるコンテンツの識別情報を読み込む手段と、

コンテンツに挿入された電子透かしを検査する電子透かし検査手段と、

コンテンツを直交変換する直交変換手段と、

直交変換後のコンテンツを量子化及びハフマン符号化する符号化圧縮手段と、

前記符号化圧縮されたコンテンツを暗号化する暗号化手段と、

コンテンツの外部機器への該暗号化コンテンツのコピー動作を制御するコピー制御手段と、

を具備し、

前記コピー制御手段は、コピー対象となるコンテンツの識別情報とコンテンツの直交変換値又はそのハッシュ値を基に外部サーバに問合せを行い、該問合せ結果に応じて、該暗号化コンテンツのコピー動作を実行するか、又は、前記電子透かし検査手段による該コンテンツの検査結果に応じて該暗号化コンテンツのコピー動作を制御することを特徴とする情報処理装置である。

【 0 0 4 7 】

また、本発明の第 1 1 の側面は、コンテンツの外部機器へのコピー動作を実行する情報処理方法であって、

コピー対象となるコンテンツを読み込むステップと、

コピー対象となるコンテンツの識別情報を読み込むステップと、

コンテンツを直交変換する直交変換ステップと、

直交変換後のコンテンツを量子化及びハフマン符号化する符号化圧縮ステップと、

前記符号化圧縮されたコンテンツを暗号化する暗号化ステップと、

コピー対象となるコンテンツの識別情報とコンテンツの直交変換値又はそのハッシュ値を基に外部サーバに問合せを行うステップと、

該問合せ結果に応じて、該暗号化コンテンツのコピー動作を実行するか、又は、コンテンツ中に挿入された電子透かしの検査結果に応じて該暗号化コンテンツのコピー動作を制御するステップと、
を具備することを特徴とする情報処理方法である。

【 0 0 4 8 】

【作用】

本発明では、コンテンツの複製を行う計算機システム自体がスクリーニング（Screening）すなわち電子透かしの検出を必ずしも行わず、別の手段により、コンテンツのコピー制御情報を取得できるようにした。例えば、コンテンツには電子透かしが挿入されていないことがあらかじめ分かっているCDからコピーするような場合には、かかるCDであることを確認できれば、電子透かしの検出処理そのものをスキップして、コピー操作全体の所要時間を短縮化することができる。

【 0 0 4 9 】

すなわち、本発明によれば、データから電子透かしを検出する必要がないので処理時間が短縮化され、ユーザの利便性が向上する。

【 0 0 5 0 】

また、電子透かしを検出する場合であっても、コンテンツ（例えば楽曲）全体にわたって検出する必要がないので、処理時間が短縮化され、ユーザの利便性が向上する。

【 0 0 5 1 】

本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。

【 0 0 5 2 】

【発明の実施の形態】

以下、図面を参照しながら本発明の実施例を詳解する。

【 0 0 5 3 】

図2には、本発明の実施例に係るコンテンツ・コピー管理システム1の全体構成を模式的に示している。

【0054】

このコンテンツ・コピー管理システム1は、音楽などのコンテンツを携帯型機器20にコピーする情報処理端末10と、情報処理端末10に対してコンテンツに関する電子透かし検出処理の代行業務を提供するサーバ30とで構成される。ここで言う、携帯型機器とは、圧縮暗号化されたデータ・コンテンツを伸張及び解読処理してコンテンツ再生する機能を持つポータブル・デバイス／プレーヤである。

【0055】

情報処理端末10は、例えば、家庭内に設置されるパーソナル・コンピュータ(PC)上に所定のアプリケーションを起動するという形態で実現される(後述)。パーソナル・コンピュータは、例えば米IBM社のPC/AT互換機及びその後継機である。

【0056】

情報処理端末10は、サーバ30とは認証を行い、安全な通信路が確保されているものとする。

【0057】

情報処理端末10は、CD-ROMドライブ(図示しない)に装填したCDから音楽データを読み出して、携帯型機器20へのコピーを行う。

【0058】

CDから読み出した音楽データは、ハード・ディスク(図示しない)上にWAV形式ファイルとして一時保存される。

【0059】

また、CDからの音楽データ読み出しの際に、楽曲に対して一意に割当られる識別情報ISRC(International Standard Recording Code)を、TOC(Table Of Contents)領域から取り出す。

【0060】

音楽データを他の機器やメディアにコピーする際にScreeningすなわち電子透かし情報の検査を行うことがSDMI(Secure Digital Music Interactive)により規定されている(前述)。但し、本実施例では、情報処理端末10

は、Screening処理を開始する前に、サーバ30に対して電子透かし情報の問合せを行う。この問合せには、対象となる楽曲のISRC（又はコンテンツを識別可能なその他の情報）を含ませておく。

【0061】

サーバ30は、各楽曲に関する電子透かし情報をデータベース管理しており、ISRCで各楽曲のエントリを検索することができるようになっている。したがって、情報処理端末10側から問合せを受け取ると、それに含まれているISRCを基に、当該楽曲のエントリの照合を試みる。そして、照合結果を要求元の情報処理端末10側に戻す。

【0062】

問合せに対する応答を受け取った情報処理端末10は、その照合結果に応じて処理を進める。例えば、電子透かし入りのメディアでない旨の結果を受け取った場合には、Screeningを行っても意味がないので、電子透かしの検出処理をスキップして、携帯型機器への音楽コンテンツのコピーを開始することができる。

【0063】

また、上述のようにISRCを用いる場合、情報処理端末10上でCD-ROMドライブからISRCを読み出す際に、途中の経路を改竄して、電子透かし入りでない別のISRC（又はコピー可であることが既に分かっている別のCDのISRC）と置換されてしまう危険がある。そこで、サーバ30に対する問合せにISRCだけでなく、例えば全体の演奏時間などメディア上のデータ・コンテンツ自体に関する他の情報を付加するようにして、なりすましの危険を排除することもできる。但し、ISRCなどの識別情報が、メディアから安全に取得する技術が存在するならば、このような属性情報を送信しなくてもよい。

【0064】

また、音楽の一部を切りとってそのデータをサーバ30に送ったり、さらに楽曲中の2以上の場所からサンプリングして、それらをサーバ30に送って照合するということも可能である。サンプルする場所を毎回ランダムに変更して特定できないようにすることで、なりすましを排除することができる。

【 0 0 6 5 】

また、音楽のサンプルを直接照合しようとすると比較的大きなデータ量になる可能性があり、通信負荷を増大させてしまいかねない。そこで、音楽データの一部又は全部を攪乱したハッシュ値をとり、その値をサーバ30側に転送して照合することで電子透かしの有無を確認するようにしてもよい。（ハッシュ関数は、デジタル署名などにも利用されるものであり、ハッシュ関数に入れるデータの一部でも改竄された場合には結果が大きく異なる性質を持つので、推測が難しく、容易に改竄を検出することができる。また、一方向性関数の特性を有するので、結果に合わせた改竄も難しい（周知）。）

【 0 0 6 6 】

あるいは、音楽データ中から特定の特徴値または特徴量を演算して、これをサーバ30において照合する手法も挙げられる。例えば、エンベロープ値であるとか、リズムに相当する周期であるとか、スペクトルの広がり方であるとかのデータを分析して、このような演算結果をサーバ30側に転送して照合するようにしてもよい。

【 0 0 6 7 】

図2に示すようなコンテンツ・コピー管理システム1の構成及び動作特性によれば、情報処理端末10においてCDから携帯型機器20に音楽コンテンツをコピーする場合において、そもそも電子透かしを含まないCDに対する電子透かし検出処理が省略されるので、利便性が高まる。

【 0 0 6 8 】

次いで、本発明の第1の実施形態に係るコンテンツ・コピー管理システム1において、情報処理端末10上でCD上の音楽データを携帯型機器20にコピーするときの処理手順について説明する。上述したように、この実施形態によれば、情報処理端末10は、サーバ30側のデータベースに対して問合せを行うことによって、電子透かしの検出処理を省略することができる。

【 0 0 6 9 】

図3には、情報処理端末10上で実行する処理手順をフローチャートの形式で示している。以下、このフローチャートに従って説明する。

【 0 0 7 0 】

まず、CD-ROMドライブ（図示しない）に装填されたCDから、ISRC（International Standard Recording Code）若しくはこれと同等のコンテンツ識別情報を取得する（ステップS1）。

【 0 0 7 1 】

一般に、CDにはTOC（Table Of Contents）のようなデータ領域が確保されており、ISRCやその他のコンテンツ属性情報を記録できるようになっている。ISRCは、12桁の数字及びアルファベット文字で構成された、CDのタイトル毎に割り振られる固有の識別情報である。

【 0 0 7 2 】

次いで、CDから所望の楽曲データを読み込んで、端末10内のハード・ディスク（図示しない）にコピーしておく（ステップS2）。

【 0 0 7 3 】

次いで、ハード・ディスク上の楽曲データから、その属性情報を取得する（ステップS3）。ここで言う属性情報とは、例えば、楽曲全体の演奏時間や、楽曲から演算して取り出した特定の特徴値（量）などである。特徴値は、エンベロープ値やリズムに相当する周期、スペクトルの広がり方などの分析値などでよい。かかる属性情報は、ISRC以外の補完的な識別情報として用いられ、不正ユーザによる「なりすまし」を防止することができる。但し、ISRCなどの識別情報をメディアから安全に取り出す手法が確立されている場合には、属性情報を使用する必要はない。

【 0 0 7 4 】

次いで、問合せ先となるサーバ30と接続し（ステップS4）、さらにサーバ30と認証及び鍵交換を行うことにより（ステップS5）、サーバ30との安全な通信路を確保する。

【 0 0 7 5 】

認証には、共通鍵あるいは公開鍵を用いた認証方式を採用することができるが、そのプロトコルはISO（International Organization for Standardization）で既に標準化されている。一方の装置から認証の要求を発行する際に乱数列も

送出し、他方の装置はその乱数を所定の鍵で暗号化して返信する。一方の装置では、これを所定の鍵で解き、元の乱数と一致するかどうかを見ることで、相手が共通の鍵又は信頼できる鍵を保持しているか、言い換えれば正しい相手か否かを認証することができる。

【 0 0 7 6 】

安全な通信路が確立した後、情報処理端末 1 0 は、ステップ S 1 において読み込んだ I S R C コードと、ステップ S 3 において取得した属性情報とをサーバ 3 0 側に転送して、C D の調査を要求する（ステップ S 6）。

【 0 0 7 7 】

C D 調査要求に対して、サーバ 3 0 側では、I S R C コードを基に自身のデータベースを検索して、そのレコードが存在するか、さらには属性情報が一致するか否かを判別して、その結果を情報処理端末 1 0 側に返す（ステップ S 7）。但し、サーバ 3 0 側で行う処理については、後に詳解する。

【 0 0 7 8 】

情報処理端末 1 0 側では、サーバ 3 0 側からの返答を基に、楽曲データの携帯型機器 2 0 へのコピーが許されるか否かを判別する。

【 0 0 7 9 】

返答内容が、データベース中に該当するレコードが存在することを示していれば（ステップ S 8）、装填中の C D はデータベース登録されたものであり、電子透かしにより挿入されたデータは既知であるから、Screening すなわち電子透かしの検出処理を省略することができる。この場合、C D からのコピーの可否判断のみを行う（ステップ S 9、S 1 0）。登録 C D は 1 回のみコピーが許容されているとすれば、ステップ S 9 において、装填中のメディアが C D - R か否かをチェックすればよい。

【 0 0 8 0 】

コピー可能であれば、ステップ S 9 1 に進んで、LCM による楽曲データの圧縮（A T R A C 3 による帯域圧縮）及び暗号化を行ってから、携帯型機器 2 0 へのコピーを行う。これに対し、コピー不可であれば、ステップ S 9 2 に進み、コピー処理を中止する。

【 0 0 8 1 】

他方、ステップ S 8 において、サーバ 3 0 側のデータベースに該当レコードが存在しない、すなわち装填中の C D が登録 C D ではないと判定された場合には、Screening すなわち電子透かし検出処理を行うより他ない（ステップ S 1 3）。

【 0 0 8 2 】

電子透かし検出を行いコピーの可否を判断した結果、コピー可能であれば L C M による楽曲の圧縮（A T R A C 3 などによる帯域圧縮）及び暗号化を行ってから、携帯型機器 2 0 へのコピーを行う（ステップ S 1 4 → S 1 1）。また、コピー不可であれば、ステップ S 1 5 に進み、コピー処理を中止する。

【 0 0 8 3 】

なお、音楽データを読み出す C D - R O M ドライブが充分信用できるものである場合（あるエンティティにより所定の安全性を保つことが認定されている場合など）、該ドライブと情報処理端末 1 0 本体が認証及び鍵交換を行うことにより、I S R C データや正常な C D であることが安全に通知できる仕組みを備えていることがより好ましい。

【 0 0 8 4 】

また、図 4 には、図 3 に示すような処理手順を実行する情報処理端末 1 0 からの問合せに対するサーバ 3 0 側が行う処理手順をフローチャートの形式で示している。以下、このフローチャートに従って説明する。

【 0 0 8 5 】

まず、クライアントすなわち情報処理端末 1 0 側からの接続要求に応答して（ステップ S 2 1）、接続処理を行う（ステップ S 2 2）。さらに、情報処理端末 1 0 と認証及び鍵交換を行うことにより（ステップ S 2 3）、情報処理端末 1 0 との安全な通信路を確保する（同上）。

【 0 0 8 6 】

次いで、情報処理端末 1 0 側から送られてくる照合データを受信する（ステップ S 2 4）。照合データには、楽曲に関する I S R C コードと属性情報が含まれている。また、ここで言う属性情報とは、楽曲全体の演奏時間や、エンベロープ

値やリズムに相当する周期、スペクトルの広がり方などの分析値などの楽曲から取り出された特徴値である。

【 0 0 8 7 】

サーバ 3 0 は、受信データ中に I S R C が含まれているか否かをチェックして（ステップ S 2 5）、I S R C が含まれる場合には I S R C からデータベースを検索し（ステップ S 2 6）、含まれていなければデータベースを全数一致検索して、特徴値などの属性情報が一致するレコードを探し出す（ステップ S 2 7）。

【 0 0 8 8 】

データベースを検索した結果、照合データと一致するレコードがデータベース中から発見できたか否かを判別する（ステップ S 2 8）。

【 0 0 8 9 】

一致するレコードが存在する場合には、付加データを付けてその旨を情報処理端末 1 0 側に返す（ステップ S 2 9）。付加データには、コピー制御情報（例えば「CD-Rからのコピー不可」など）を含めることができる。

【 0 0 9 0 】

他方、一致するレコードが存在しない場合には、その旨を情報処理端末 1 0 側に返す（ステップ S 3 0）。

【 0 0 9 1 】

そして、情報処理端末 1 0 との接続を解除して（ステップ S 3 1）、本処理ルーチン全体を終了する。

【 0 0 9 2 】

図 3 及び図 4 に示す例では、情報処理端末 1 0 は、サーバ 3 0 側に対して装填中の CD が登録済み CD であるか否かのみを問合せ、コピー可能であるか否かは情報処理端末 1 0 側で判断するようになっている（図 3 のステップ S 9 及び S 1 0）。これに対し、サーバ 3 0 は、情報処理端末 1 0 側からの問合せに応答して、さらにコピーの可否まで判断して返答することもできる。

【 0 0 9 3 】

図 5 及び図 6 には、後者の場合における情報処理端末 1 0 及びサーバ 3 0 側が行う処理手順をそれぞれフローチャートの形式で示している。以下、これらフロ

ーチャートに従って説明する。

【0094】

情報処理端末10側では、まず、CD-ROMドライブ（図示しない）に装填されたCDから、ISRC（International Standard Recording Code）若しくはこれと同等のコンテンツ識別情報を取得する（ステップS41）。

【0095】

次いで、CDから所望の楽曲データを読み込んで、端末10内のハード・ディスク（図示しない）にコピーしておく（ステップS42）。

【0096】

次いで、ハード・ディスク上の楽曲データから、その属性情報を取得する（ステップS43）。ここで言う属性情報とは、例えば、楽曲全体の演奏時間や、楽曲から演算して取り出した特定の特徴値（量）などである。特徴値は、エンベロープ値やリズムに相当する周期、スペクトルの広がり方などの分析値などでよい。かかる属性情報は、ISRC以外の補完的な識別情報として用いられ、不正ユーザによる「なりすまし」を防止することができる。但し、ISRCのような識別情報をメディアから安全に引き出す手法が確立されていれば、このような属性情報を使用する必要はない。

【0097】

次いで、問合せ先となるサーバ30と接続し（ステップS44）、さらにサーバ30と認証及び鍵交換を行うことにより（ステップS45）、サーバ30との安全な通信路を確保する。

【0098】

そして、情報処理端末10は、ISRCコード及び属性情報をサーバ30側に転送して、コピー可否の判断を要求する（ステップS46）。判断のために、装填中のCDがCD-Rか否かなどの付随情報も併せて送信する。

【0099】

コピー可否の判断要求に対して、サーバ30側では、ISRCコードを基に自身のデータベースを検索して、そのレコードが存在するか、さらには属性情報が一致するか否かなどを判別して、判断結果を情報処理端末10側に返す（ステッ

プ S 4 7)。但し、サーバ 3 0 側で行う処理については、後に詳解する。

【 0 1 0 0 】

情報処理端末 1 0 側では、サーバ 3 0 側からの返答を基に、楽曲データの携帯型機器 2 0 へのコピーが許されるか否かを判別する（ステップ S 4 8）。

【 0 1 0 1 】

サーバ 3 0 による判断結果が「コピー可」であれば、ステップ S 4 9 に進んで、LCM による楽曲の圧縮及び暗号化を行ってから、携帯型機器 2 0 へのコピーを行う。

【 0 1 0 2 】

また、サーバ 3 0 による判断結果が「コピー不可」であれば、ステップ S 5 0 に進み、コピー処理を中止する。

【 0 1 0 3 】

また、サーバ 3 0 による判断結果が「Screening 実行」であれば、電子透かし検出処理を行う他ない（ステップ S 5 1）。電子透かし検出を行いコピーの可否を判断した結果、コピー可能であれば LCM による楽曲の圧縮（ATRAC 3 などによる帯域圧縮）及び暗号化を行ってから、携帯型機器 2 0 へのコピーを行う（ステップ S 5 2 → S 4 9）。また、コピー不可であれば、ステップ S 5 3 に進み、コピー処理を中止する。

【 0 1 0 4 】

他方、サーバ 3 0 側では、クライアントすなわち情報処理端末 1 0 側からの接続要求に応答して（ステップ S 6 1）、接続処理を行う（ステップ S 6 2）。さらに、情報処理端末 1 0 と認証及び鍵交換を行うことにより（ステップ S 6 3）、情報処理端末 1 0 との安全な通信路を確保する。

【 0 1 0 5 】

次いで、情報処理端末 1 0 側から送られてくる照合データを受信する（ステップ S 6 4）。照合データには、楽曲に関する ISRC コードと属性情報が含まれている。また、ここで言う属性情報とは、楽曲全体の演奏時間や、エンベロープ値やリズムに相当する周期、スペクトルの広がり方などの分析値などの楽曲から取り出された特徴値である。また、情報処理端末 1 0 において現在装填中の CD

がCD-Rか否かなどの付随データも併せて受信する。

【0106】

サーバ30は、受信データ中にISRCが含まれているか否かをチェックして（ステップS65）、ISRCが含まれる場合にはISRCからデータベースを検索し（ステップS66）、含まれていなければデータベースを全数一致検索して、特徴値などの属性情報が一致するレコードを探し出す（ステップS67）。

【0107】

データベースを検索した結果、照合データと一致するレコードがデータベースの中から発見できたか否かを判別する（ステップS68）。

【0108】

一致するレコードが存在する場合には、レコード内の記述などを基に、CDからのコピーの可否を判断する（ステップS69）。また、情報処理端末10側から送られてきた、「CD-Rか否か」などの付加データを参考にしてコピーの可否を判断してもよい。

【0109】

コピー可能であれば、情報処理端末10に対して「コピー可」を返し（ステップS70）、コピー不可であれば、情報処理端末に対して「コピー不可」を返す（ステップS72）。

【0110】

また、データベース上にレコードが存在しない場合には（ステップS68）、情報処理端末10においてScreening処理を省略することは許されないもので、情報処理端末に対して「Screening実行」を返す（ステップS73）。

【0111】

そして、情報処理端末10との接続を解除して（ステップS71）、本処理ルーチン全体を終了する。

【0112】

図7には、サーバ30側のデータベースに対して問合せを行うことによって電子透かし検出処理を省略するための、情報処理端末10上で実行する処理手順の

さらに他の例をフローチャートの形式で示している。

【0113】

データベースに対する照合処理のために、ISRCしか使用しない場合には、CD-ROMドライブからISRCを読み出す際に、途中の経路を改竄して、電子透かし入りでない別のISRC（又はコピー可であることが分かっている別のCDのISRC）と置換されてしまう危険がある。そこで、図7に示す例では、楽曲のデータの一部を参照することで、CDであるか否かを照合するようにしている。以下、フローチャートに従って説明する。

【0114】

まず、CD-ROMドライブ（図示しない）に装填されたCDから、ISRC（International Standard Recording Code）若しくはこれと同等のコンテンツ識別情報を取得する（ステップS81）。

【0115】

次いで、CDから所望の楽曲データを読み込んで、端末10内のハード・ディスク（図示しない）にコピーしておく（ステップS82）。

【0116】

次いで、ハード・ディスク上の楽曲データから、ランダムに1箇所又は数カ所のデータのある秒数だけ選択して実データを取り出すとともに、そのデータ位置情報（先頭から何バイト目か、あるいは演奏時間上何秒目かなど）を、属性情報取得する（ステップS83）。実データを取り出す場所は固定であってもよいが、不正ユーザによるデータ置換の危険を排除するにはランダムな場所であることが好ましい。

【0117】

次いで、問合せ先となるサーバ30と接続し（ステップS84）、さらにサーバ30と認証及び鍵交換を行うことにより（ステップS85）、サーバ30との安全な通信路を確保する。

【0118】

そして、情報処理端末10は、ステップS81において読み込んだISRCコードと、ステップS83において取得した属性情報とをサーバ30側に転送して

、CDの調査を要求する（ステップS 8 6）。

【0 1 1 9】

CD調査要求に対して、サーバ3 0 側では、I S R Cコードを基に自身のデータベースを検索して、そのレコードが存在するか、さらには属性情報（すなわち楽曲の一部を切り出したデータ）が一致するか否かを判別して、その結果を情報処理端末1 0 側に返す（ステップS 8 7）。調査要求に対してサーバ3 0 側において実行すべき処理手順は、属性情報ではなく切り出した実データの一部をデータベースで照合するという点以外は図4 に示したものと同様なので、ここでは説明を省略する。

【0 1 2 0】

情報処理端末1 0 側では、サーバ3 0 側からの返答を基に、楽曲データの携帯型機器2 0 へのコピーが許されるか否かを判別する。

【0 1 2 1】

返答内容が、データベース中に該当するレコードが存在することを示していれば（ステップS 8 8）、装填中のCDはデータベース登録されたものであり、電子透かしにより挿入されたデータは既知であるから、Screeningすなわち電子透かしの検出処理を省略することができる。この場合、CDからのコピーの可否判断のみを行う（ステップS 8 9、S 9 0）。登録CDは1 回のみコピーが許容されているとすれば、ステップS 8 9において、装填中のメディアがCD-Rか否かをチェックすればよい。

【0 1 2 2】

コピー可能であれば、ステップS 9 1に進んで、LCMによる楽曲データの圧縮（ATRAC3による帯域圧縮）及び暗号化を行ってから、携帯型機器2 0 へのコピーを行う。これに対し、コピー不可であれば、ステップS 1 2に進み、コピー処理を中止する。

【0 1 2 3】

他方、ステップS 8 8において、サーバ3 0 側のデータベースに該当レコードが存在しない、すなわち装填中のCDが登録CDではないと判定された場合には、Screeningすなわち電子透かし検出処理を行うより他ない（ステップ

S93)。

【0124】

電子透かし検出を行いコピーの可否を判断した結果、コピー可能であればLCMによる楽曲の圧縮(ATRAC3などによる帯域圧縮)及び暗号化を行ってから、携帯型機器20へのコピーを行う(ステップS94→S91)。また、コピー不可であれば、ステップS95に進み、コピー処理を中止する。

【0125】

図8には、サーバ30側のデータベースに対して問合せを行うことによって電子透かし検出処理を省略するための、情報処理端末10上で実行する処理手順のさらに他の例をフローチャートの形式で示している。

【0126】

図8に示す例では、楽曲のデータの全部(又は一部でも可)をハッシュ関数にかけて得られたハッシュ値を参照することで、CDであるか否かを照合するようにしている。

【0127】

ここで、ハッシュ関数とは、データ列を圧縮して別のデータ列に置き換えるものである。一般に、ハッシュ関数に入れるデータの一部でも改竄された場合には結果が大きく異なる性質を持つので、推測が難しく、容易に改竄を検出することができる。また、一方向性関数の特性を有するので、結果に合わせた改竄も難しい(周知)。現在、SHA-1と呼ばれるアルゴリズムが公開されている。

【0128】

以下、図8に示すフローチャートに従って説明する。

【0129】

まず、CD-ROMドライブ(図示しない)に装填されたCDから、ISRC(International Standard Recording Code)若しくはこれと同等のコンテンツ識別情報を取得する(ステップS101)。

【0130】

次いで、CDから所望の楽曲データを読み込んで、端末10内のハード・ディスク(図示しない)にコピーしておく(ステップS102)。

【0131】

次いで、ハード・ディスク上の楽曲データ全体をハッシュ関数にかけてそのハッシュ値を計算して、これを属性情報として一時的に保持する（ステップS103）。

【0132】

次いで、問合せ先となるサーバ30と接続し（ステップS104）、さらにサーバ30と認証及び鍵交換を行うことにより（ステップS105）、サーバ30との安全な通信路を確保する。

【0133】

そして、情報処理端末10は、ステップS101において読み込んだISRCコードと、ステップS103において計算したハッシュ値とをサーバ30側に転送して、CDの調査を要求する（ステップS106）。

【0134】

CD調査要求に対して、サーバ30側では、ISRCコードを基に自身のデータベースを検索して、そのレコードが存在するか、さらにはそのハッシュ値が一致するか否かを判別して、その結果を情報処理端末10側に返す（ステップS107）。

【0135】

図8に示す例ではデータ全体のハッシュ値をサーバ30に送信して照合するので、図7に示した場合とは相違し、楽曲全体にわたって改竄されていないかどうかを検査することができ、CDのデータに対してすり替えやその他の何らかの不正な処理が印加されていないかどうかを確認することができる。また、ハッシュ値を送るので、楽曲全体にわたるデータを送信するための通信負荷が軽くて済む。サーバ30側でも、楽曲全体ではなくそのハッシュ値だけを保管しておけばよいので、記憶容量を節約することができる。例えばSHA-1では、512ビットごとに160ビットのデータを出力するようになっているので、これを累積計算することで、楽曲全体のハッシュ値を得ることができる。

【0136】

情報処理端末10側では、サーバ30側からの返答を基に、楽曲データの携帯

型機器 2 0 へのコピーが許されるか否かを判別する。

【 0 1 3 7 】

返答内容が、データベース中に該当するレコードが存在することを示していれば（ステップ S 1 0 8）、装填中の CD はデータベース登録されたものであり、電子透かしにより挿入されたデータは既知であるから、Screening すなわち電子透かしの検出処理を省略することができる。この場合、CD からのコピーの可否判断のみを行う（ステップ S 1 0 9、S 1 1 0）。登録 CD は 1 回のみコピーが許容されているとすれば、ステップ S 1 0 9 において、装填中のメディアが CD-R か否かをチェックすればよい。

【 0 1 3 8 】

コピー可能であれば、ステップ S 1 1 1 に進んで、LCM による楽曲データの圧縮（ATRAC3 による帯域圧縮）及び暗号化を行ってから、携帯型機器 2 0 へのコピーを行う。これに対し、コピー不可であれば、ステップ S 1 1 2 に進み、コピー処理を中止する。

【 0 1 3 9 】

他方、ステップ S 1 0 8 において、サーバ 3 0 側のデータベースに該当レコードが存在しない、すなわち装填中の CD が登録 CD ではないと判定された場合には、Screening すなわち電子透かし検出処理を行うより他ない（ステップ S 1 1 3）。

【 0 1 4 0 】

電子透かし検出を行いコピーの可否を判断した結果、コピー可能であれば LCM による楽曲の圧縮（ATRAC3 などによる帯域圧縮）及び暗号化を行ってから、携帯型機器 2 0 へのコピーを行う（ステップ S 1 1 4 → S 1 1 1）。また、コピー不可であれば、ステップ S 1 1 5 に進み、コピー処理を中止する。

【 0 1 4 1 】

これまでに説明した実施形態ではいずれも、情報処理端末 1 0 は、CD から読み込んだ楽曲がコピー可能であることを確認できた後に、データ・コンテンツの圧縮暗号化及び携帯型機器 2 0 へのコピー処理に移行するものである。これに対し、データ・コンテンツの圧縮暗号化処理の一部でコピー可否の確認処理を行う

こともできる。

【 0 1 4 2 】

図 9 には、LCM での帯域圧縮過程のデータをデータベースに対する照合データとして用いることができるコンテンツ・コピー管理システム 1 - 2 の構成例を示し、また、図 1 0 には、該システム 1 - 2 において情報処理端末 1 0 が実行する処理手順をフローチャートの形式で示している。

【 0 1 4 3 】

データ圧縮プロセスは、一般に、D C T (Discrete Cosine Transform: 離散コサイン変換)、量子化、及びハフマン符号化で構成される。M P 3 (MPEG-1 Audio Layer-III) や A T R A C などの帯域圧縮では m D C T (変形離散コサイン変換) が用いられている。m D C T は、直交変換の 1 つであり、時間軸領域を周波数領域に変換する。また、直交変換には、m D C T 以外にも、D C T (離散コサイン変換)、w a v e l e t ("w a v e l e t" は米サマス・テクノロジーズ社が開発した波形分析技術) などがある

【 0 1 4 4 】

この実施形態に係るシステム 1 - 2 では、情報処理端末 1 0 は、LCM プロセスにおいて生成された m D C T 係数のハッシュ値を求めて、これをサーバ 3 0 側に転送してデータベースと照合するようになっている。

【 0 1 4 5 】

データベースと照合した結果、コピー可であれば、そのまま圧縮及び暗号処理を進めて、携帯型機器 2 0 へのデータ・コピーを行う。他方、コピー不可と判断された場合には、S c r e e n i n g 処理に戻って、電子透かし検出を行い、その検出結果に従ってコピーの可否を再度判断する。

【 0 1 4 6 】

本実施形態によれば、情報処理端末 1 0 は、S c r e e n i n g 処理が完了していなくても、コピー用データの圧縮などの処理を並行して行うことができるので、コピー処理全体に要する時間が短縮化される。また、圧縮・暗号化されたコピー用データを作成しても、コピー不可と判断されたときには最終的に携帯型機器 2 0 へのコピーを行わなければコンテンツ保護上も問題はない。また、m D C

Tなどの圧縮過程でのデータは、通常、PCM (Pulse Code Modulation) データよりもデータ量が少ないので、照合用データとしては都合がよい。

【0147】

以下、図10に示すフローチャートを参照しながら、情報処理端末10において実行される処理手順について説明する。

【0148】

まず、CD-ROMドライブ（図示しない）に装填されたCDから、ISRC (International Standard Recording Code) 若しくはこれと同等のコンテンツ識別情報を取得する（ステップS121）。

【0149】

次いで、CDから所望の楽曲データを読み込んで、端末10内のハード・ディスク（図示しない）にコピーしておく（ステップS122）。

【0150】

次いで、LCD処理の第1段階としてmDCTを実行して、楽曲データのmDCT係数を計算する（ステップS123）。さらに、mDCT係数をハッシュ関数にかけてそのハッシュ値を計算する（ステップS124）。

【0151】

次いで、問合せ先となるサーバ30と接続し（ステップS125）、さらにサーバ30と認証及び鍵交換を行うことにより（ステップS126）、サーバ30との安全な通信路を確保する。

【0152】

そして、情報処理端末10は、ステップS121において読み込んだISRCコードと、ステップS124において計算したハッシュ値とをサーバ30側に転送して、CDの調査を要求する（ステップS127）。

【0153】

CD調査要求に対して、サーバ30側では、ISRCコードを基に自身のデータベースを検索して、そのレコードが存在するか、さらにはそのハッシュ値が一致するか否かを判別して、その結果を情報処理端末10側に返す（ステップS128）。

【 0 1 5 4 】

情報処理端末 1 0 側では、サーバ 3 0 側からの返答を基に、楽曲データの携帯型機器 2 0 へのコピーが許されるか否かを判別する。

【 0 1 5 5 】

返答内容が、データベース中に該当するレコードが存在することを示していれば（ステップ S 1 2 9）、装填中の C D はデータベース登録されたものであり、電子透かしにより挿入されたデータは既知であるから、Screening すなわち電子透かしの検出処理を省略することができる。この場合、C D からのコピーの可否判断のみを行う（ステップ S 1 3 0、S 1 3 1）。登録 C D は 1 回のみコピーが許容されているとすれば、ステップ S 1 3 0 において、装填中のメディアが C D - R か否かをチェックすればよい。

【 0 1 5 6 】

コピー可能であれば、量子化及びハフマン符号化という圧縮処理の残りの過程を実行する（ステップ S 1 3 2）。そして、圧縮データをさらに暗号化して携帯型機器 2 0 へのコピーを行う（ステップ S 1 3 3）。これに対し、コピー不可であれば、ステップ S 1 3 4 に進み、コピー処理を中止する。

【 0 1 5 7 】

他方、ステップ S 1 2 9 において、サーバ 3 0 側のデータベースに該当レコードが存在しない、すなわち装填中の C D が登録 C D ではないと判定された場合には、Screening すなわち電子透かし検出処理を行う他ない（ステップ S 1 3 5）。

【 0 1 5 8 】

電子透かし検出を行いコピーの可否を判断した結果、コピー可能であれば、量子化及びハフマン符号化という圧縮処理の残りの過程を実行する（ステップ S 1 3 2）。そして、圧縮データをさらに暗号化して携帯型機器 2 0 へのコピーを行う（ステップ S 1 3 3）。また、コピー不可であれば、ステップ S 1 3 7 に進み、コピー処理を中止する。

【 0 1 5 9 】

上述したような情報処理端末 1 0 における音楽データのコピー機能を、専用の

ハードウェア構成を備えた端末装置によって実現することも可能であるが、汎用的な処理が可能な一般的な計算機システム上で、図 3、図 5、図 7、図 10 の各フローチャートで示した処理手順をコンピュータ可読形式で記述したコンテンツ・コピー・アプリケーションを実行するという形態でも、本発明を実装することができる。

【0160】

図 11 には、本発明に係る情報処理端末 10 を実現することができる計算機システム 100 のハードウェア構成を模式的に示している。以下、同図を参照しながら、システム 100 内の各構成要素について説明する。

【0161】

システム 100 のメイン・コントローラである CPU (Central Processing Unit) 101 は、オペレーティング・システム (OS) の制御下で、各種のアプリケーションを実行する。CPU 101 は、例えば、図 3、図 5、図 7、図 10 の各フローチャートで示した処理手順をコンピュータ可読形式で記述したコンテンツ・コピー・アプリケーションを実行することができる。図示の通り、CPU 101 は、バス 108 によって他の機器類 (後述) と相互接続されている。

【0162】

メモリ 102 は、CPU 101 において実行されるプログラム・コードを格納したり、プログラム実行中の作業データを一時保管するために使用される記憶装置である。同図に示すメモリ 102 は、不揮発及び揮発メモリ双方を含むものと理解されたい。

【0163】

ディスプレイ・コントローラ 103 は、CPU 101 が発行する描画命令を実際に処理するための専用コントローラである。ディスプレイ・コントローラ 103 において処理された描画データは、例えばフレーム・バッファ (図示しない) に一旦書き込まれた後、ディスプレイ 111 によって画面出力される。

【0164】

入力機器インターフェース 104 は、キーボード 112 やマウス 113 などのユーザ入力機器を計算機システム 100 に接続するための装置である。

【0165】

ネットワーク・インターフェース105は、Ethernetなどの所定の通信プロトコルに従って、システム100をLAN (Local Area Network) などの局所的ネットワーク、さらにはインターネットのような広域ネットワークに接続することができる。

【0166】

ネットワーク上では、複数のホスト端末（図示しない）がトランスペアレントな状態で接続され、分散コンピューティング環境が構築されている。計算機システム100とサーバ30をネットワーク経由で接続することも可能であり、サーバ30に対してデータベース問い合わせを行うことができる。また、ネットワーク上では、ソフトウェア・プログラムやデータ・コンテンツなどの配信が行うことができる。例えば、図3、図5、図7、図10の各フローチャートで示した処理手順をコンピュータ可読形式で記述したコンテンツ・コピー・アプリケーションを、ネットワーク経由で計算機システム100にダウンロードすることができる。また、コピー対象となる音楽データなどを、ネットワーク経由で配信することもできる。

【0167】

外部機器インターフェース107は、ハード・ディスク・ドライブ（HDD）114やメディア・ドライブ115などの外部装置をシステム100に接続するための装置である。

【0168】

HDD114は、記憶担体としての磁気ディスクを固定的に搭載した外部記憶装置であり（周知）、記憶容量やデータ転送速度などの点で他の外部記憶装置よりも優れている。ソフトウェア・プログラムを実行可能な状態でHDD114上に置くことをプログラムのシステムへの「インストール」と呼ぶ。通常、HDD114には、CPU101が実行すべきオペレーティング・システムのプログラム・コードや、アプリケーション・プログラム、デバイス・ドライバなどが不揮発的に格納されている。

【0169】

例えば、図3、図5、図7、図10の各フローチャートで示した処理手順をコンピュータ可読形式で記述したコンテンツ・コピー・アプリケーションを、HDD 114上にインストールすることができる。また、コピー対象となる音楽データなどを、HDD 114上に一時的に保存することもできる。CDなどの記録メディアから読み出された音楽データは、例えばWAV形式のコンピュータ・ファイルとして、HDD 114上に保存される。

【0170】

メディア・ドライブ115は、CD (Compact Disc) やMO (Magneto-Optical disc)、DVD (Digital Versatile Disc) などの可搬型メディアを装填して、そのデータ記録面にアクセスするための装置である。

【0171】

可搬型メディアは、主として、ソフトウェア・プログラムやデータ・ファイルなどをコンピュータ可読形式のデータとしてバックアップすることや、これらをシステム間で移動（すなわち販売・流通・配布を含む）する目的で使用される。例えば、図3、図5、図7、図10の各フローチャートで示した処理手順をコンピュータ可読形式で記述したコンテンツ・コピー・アプリケーションを、これら可搬型メディアを利用して複数の機器間で物理的に流通・配布することができる。また、コピー対象となる音楽データなどを、これら可搬型メディアを利用して機器間で物理的に流通・配布することができる。

【0172】

図11に示すような計算機システム100の一例は、米IBM社のパーソナル・コンピュータ”PC/AT (Personal Computer/Advanced Technology)”の互換機又は後継機である。勿論、他のアーキテクチャを備えたコンピュータを、本実施形態に係る計算機システム100として適用することも可能である。

【0173】

また、上述したようなサーバ30による音楽データのコピー制御機能並びに電子透かし検出の代行機能を、専用のハードウェア構成を備えた端末装置によって実現することも可能であるが、汎用的な処理が可能な一般的な計算機システム上で、図4、図6、図8の各フローチャートで示した処理手順をコンピュータ可読

形式で記述したコンテンツ・コピー制御並びに電子透かし検出代行サーバ・アプリケーションを実行するという形態でも、本発明を実装することができる。

【 0 1 7 4 】

図 1 2 には、本発明に係るサーバ 3 0 を実現することができる計算機システム 2 0 0 のハードウェア構成を模式的に示している。以下、同図を参照しながら、システム 2 0 0 内の各構成要素について説明する。

【 0 1 7 5 】

システム 2 0 0 のメイン・コントローラである CPU (Central Processing Unit) 2 0 1 は、オペレーティング・システム (OS) の制御下で、各種のアプリケーションを実行する。CPU 2 0 1 は、例えば、図 4、図 6、図 8 の各フローチャートで示した処理手順をコンピュータ可読形式で記述したコンテンツ・コピー制御並びに電子透かし検出代行サーバ・アプリケーションを実行することができる。図示の通り、CPU 2 0 1 は、バス 2 0 8 によって他の機器類 (後述) と相互接続されている。

【 0 1 7 6 】

メモリ 2 0 2 は、CPU 2 0 1 において実行されるプログラム・コードを格納したり、プログラム実行中の作業データを一時保管するために使用される記憶装置である。同図に示すメモリ 2 0 2 は、不揮発及び揮発メモリ双方を含むものと理解されたい。

【 0 1 7 7 】

ディスプレイ・コントローラ 2 0 3 は、CPU 2 0 1 が発行する描画命令を実際に処理するための専用コントローラである。ディスプレイ・コントローラ 1 0 3 において処理された描画データは、例えばフレーム・バッファ (図示しない) に一旦書き込まれた後、ディスプレイ 2 1 1 によって画面出力される。

【 0 1 7 8 】

入力機器インターフェース 2 0 4 は、キーボード 2 1 2 やマウス 2 1 3 などのユーザ入力機器を計算機システム 2 0 0 に接続するための装置である。

【 0 1 7 9 】

ネットワーク・インターフェース 2 0 5 は、Ethernet などの所定の通

信プロトコルに従って、システム200をLAN (Local Area Network) などの局所的ネットワーク、さらにはインターネットのような広域ネットワークに接続することができる。

【0180】

ネットワーク上では、複数のホスト端末（図示しない）がトランスペアレントな状態で接続され、分散コンピューティング環境が構築されている。計算機システム200と情報処理端末10をネットワーク経由で接続することも可能であり、情報処理端末10からデータベース問い合わせを受けることができる。また、ネットワーク上では、ソフトウェア・プログラムやデータ・コンテンツなどの配信が行うことができる。例えば、図4、図6、図8の各フローチャートで示した処理手順をコンピュータ可読形式で記述したコンテンツ・コピー制御並びに電子透かし検出代行サーバ・アプリケーションを、ネットワーク経由で計算機システム200にダウンロードすることができる。また、コピー対象となる音楽データなどを、ネットワーク経由で配信することもできる。

【0181】

データベース・インターフェース207は、ハード・ディスク・ドライブ（HDD）214のようなデータベースを構築するための外部装置をシステム100に接続するための装置である。データベース214上では、各楽曲に関する電子透かし情報やコピー可否情報などがデータベース管理されており、情報処理端末10からのISRCなどの楽曲の識別情報や属性情報に基づく問い合わせに応じることができる（前述）。

【0182】

また、HDD214は、記憶担体としての磁気ディスクを固定的に搭載した外部記憶装置であり（周知）、記憶容量やデータ転送速度などの点で他の外部記憶装置よりも優れている。ソフトウェア・プログラムを実行可能な状態でHDD214上に置くことをプログラムのシステムへの「インストール」と呼ぶ。通常、HDD214には、CPU201が実行すべきオペレーティング・システムのプログラム・コードや、アプリケーション・プログラム、デバイス・ドライバなどが不揮発的に格納されている。例えば、図4、図6、図8の各フローチャートで示

した処理手順をコンピュータ可読形式で記述したコンテンツ・コピー制御並びに電子透かし検出代行サーバ・アプリケーションを、HDD 2 1 4 上にインストールすることができる。

【0 1 8 3】

図 1 2 に示すような計算機システム 2 0 0 の一例は、米 I B M 社のパーソナル・コンピュータ”P C / A T (Personal Computer/Advanced Technology)”の互換機又は後継機である。勿論、他のアーキテクチャを備えたコンピュータを、本実施形態に係る計算機システム 2 0 0 として適用することも可能である。

【0 1 8 4】

〔追補〕

以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。

【0 1 8 5】

本明細書中では、C D に記録された音楽データのコピーを行う場合を例にとって本発明の実施形態を説明したが、本発明の適用範囲はこれに限定されるものではない。例えば映像や静止画など他のデータ・コンテンツに対しても、あるいは D V D や M D など他の記録メディアから読み取ったデータに対しても、本発明は同様に作用効果を奏することができる。

【0 1 8 6】

要するに、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【0 1 8 7】

【発明の効果】

以上詳記したように、本発明によれば、コンテンツに埋め込まれた電子透かしを検査することができる、優れた電子透かし検査技術を提供することができる。

【0 1 8 8】

また、本発明によれば、コンテンツに埋め込まれた電子透かしを検査した結果

に従ってコンテンツの複製の可否を判断することができる、優れた電子透かし検査技術を提供することができる。

【0189】

また、本発明によれば、計算負荷の高い電子透かし検査処理を代行して、コンテンツの複製の可否を判断することができる、優れた電子透かし検査技術を提供することができる。

【0190】

本発明では、コンテンツの複製を行う計算機システム自体がスクリーニングすなわち電子透かしの検出を必ずしも行わず、別の手段により、コンテンツのコピー制御情報を取得できるようにした。例えば、コンテンツには電子透かしが挿入されていないことがあらかじめ分かっているCDからコピーするような場合には、かかるCDであることを確認できれば、電子透かしの検出処理そのものをスキップして、コピー所要時間を短縮化する。

【0191】

すなわち、本発明によれば、データから電子透かしを検出する必要がないので処理時間が短縮化され、ユーザの利便性が向上する。

【0192】

また、電子透かしを検出する場合であっても、コンテンツ（例えば楽曲）全体にわたって検出する必要がないので、処理時間が短縮化され、ユーザの利便性が向上する。

【図面の簡単な説明】

【図1】

SDMIで想定しているScreening処理を実現するための機能ブロック図である。

【図2】

本発明の実施例に係るコンテンツ・コピー管理システム1の全体構成を模式的に示した図である。

【図3】

本発明の第1の実施形態に係るコンテンツ・コピー管理システム1において、

情報処理端末 1 0 上で C D 上の音楽データを携帯型機器 2 0 にコピーするときの、情報処理端末 1 0 側で実行する処理手順を示したフローチャートである。

【図 4】

本発明の第 1 の実施形態に係るコンテンツ・コピー管理システム 1 において、情報処理端末 1 0 上で C D 上の音楽データを携帯型機器 2 0 にコピーするときの、サーバ 3 0 側で実行する処理手順を示したフローチャートである。

【図 5】

本発明の第 1 の実施形態に係るコンテンツ・コピー管理システム 1 において、情報処理端末 1 0 上で C D 上の音楽データを携帯型機器 2 0 にコピーするときの、情報処理端末 1 0 側で実行する処理手順の他の例を示したフローチャートである。

【図 6】

本発明の第 1 の実施形態に係るコンテンツ・コピー管理システム 1 において、情報処理端末 1 0 上で C D 上の音楽データを携帯型機器 2 0 にコピーするときの、サーバ 3 0 側で実行する処理手順の他の例を示したフローチャートである。

【図 7】

サーバ 3 0 側のデータベースに対して問合せを行うことによって電子透かし検出処理を省略するための、情報処理端末 1 0 上で実行する処理手順のさらに他の例を示したフローチャートである。

【図 8】

サーバ 3 0 側のデータベースに対して問合せを行うことによって電子透かし検出処理を省略するための、情報処理端末 1 0 上で実行する処理手順のさらに他の例を示したフローチャートである。

【図 9】

L C M での帯域圧縮過程のデータをデータベースに対する照合データとして用いることができるコンテンツ・コピー管理システム 1 - 2 の構成を模式的に示した図である。

【図 1 0】

コンテンツ・コピー管理システム 1 - 2 において情報処理端末 1 0 が実行する

処理手順を示したフローチャートである。

【図 1 1】

情報処理端末 1 0 として適用可能な計算機システム 1 0 0 の構成を模式的に示した図である。

【図 1 2】

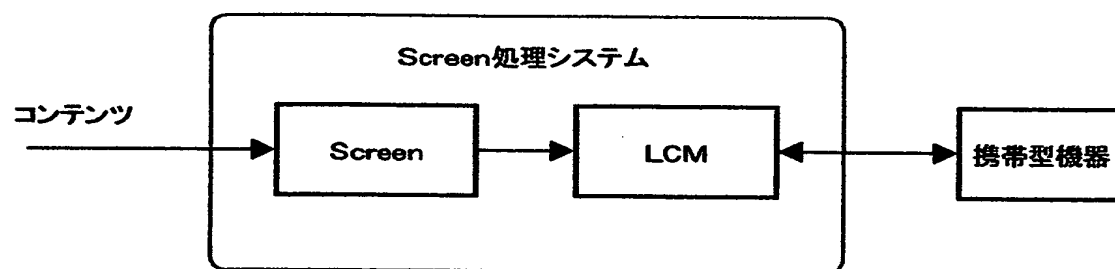
サーバ 3 0 として適用可能な計算機システム 2 0 0 の構成を模式的に示した図である。

【符号の説明】

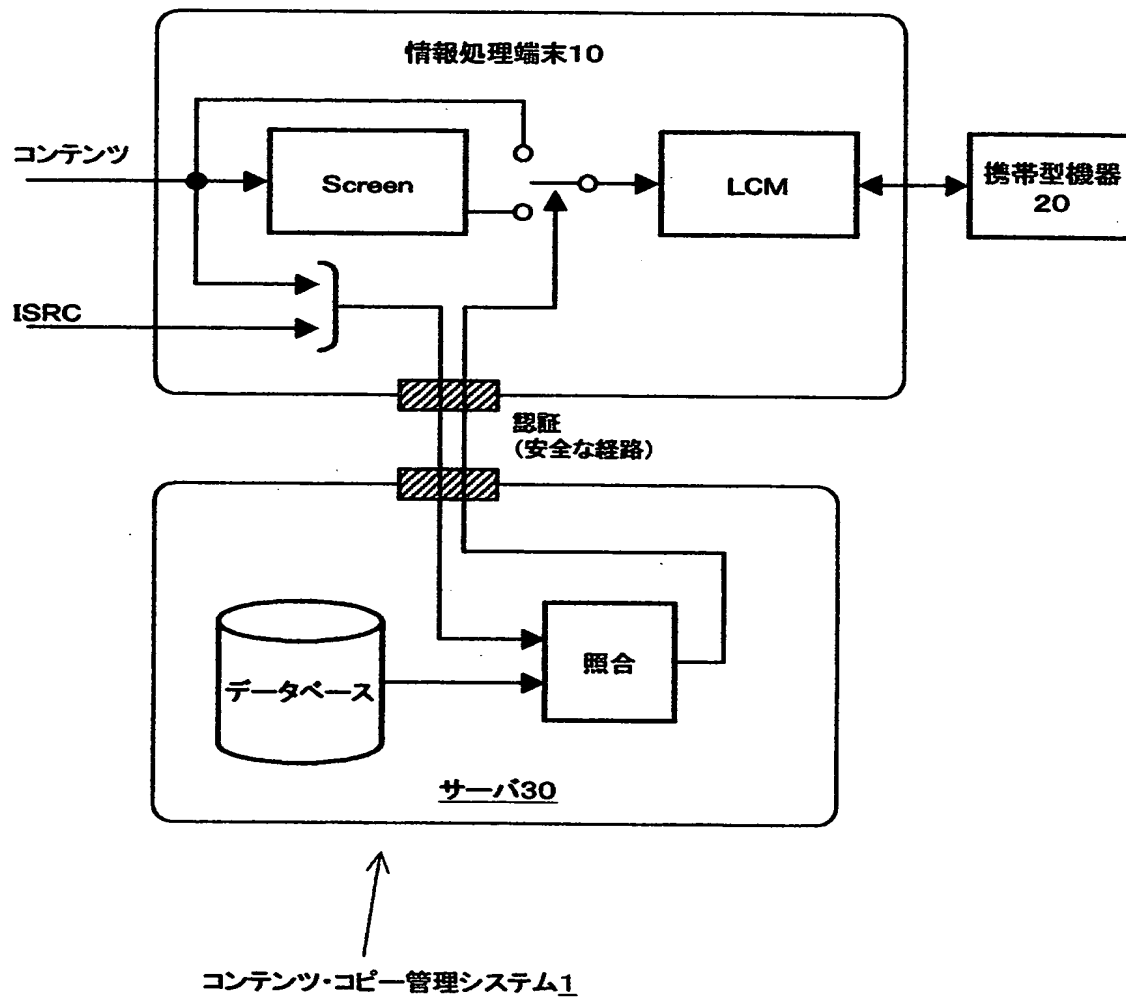
- 1 …コンテンツ・コピー管理システム
- 1 0 …情報処理端末
- 2 0 …携帯型機器
- 3 0 …サーバ
- 1 0 0 …計算機システム（情報処理端末）
- 1 0 1 …CPU, 1 0 2 …メモリ
- 1 0 3 …ディスプレイ・コントローラ
- 1 0 4 …入力機器インターフェース
- 1 0 5 …ネットワーク・インターフェース
- 1 0 7 …外部機器インターフェース, 1 0 8 …バス
- 1 1 1 …ディスプレイ, 1 1 2 …キーボード, 1 1 3 …マウス
- 1 1 4 …ハード・ディスク装置, 1 1 5 …メディア・ドライブ
- 2 0 0 …計算機システム（サーバ）
- 2 0 1 …CPU, 2 0 2 …メモリ
- 2 0 3 …ディスプレイ・コントローラ
- 2 0 4 …入力機器インターフェース
- 2 0 5 …ネットワーク・インターフェース
- 2 0 7 …データ・ベースインターフェース, 2 0 8 …バス
- 2 1 1 …ディスプレイ, 2 1 2 …キーボード, 2 1 3 …マウス
- 2 1 4 …データベース

【書類名】 図面

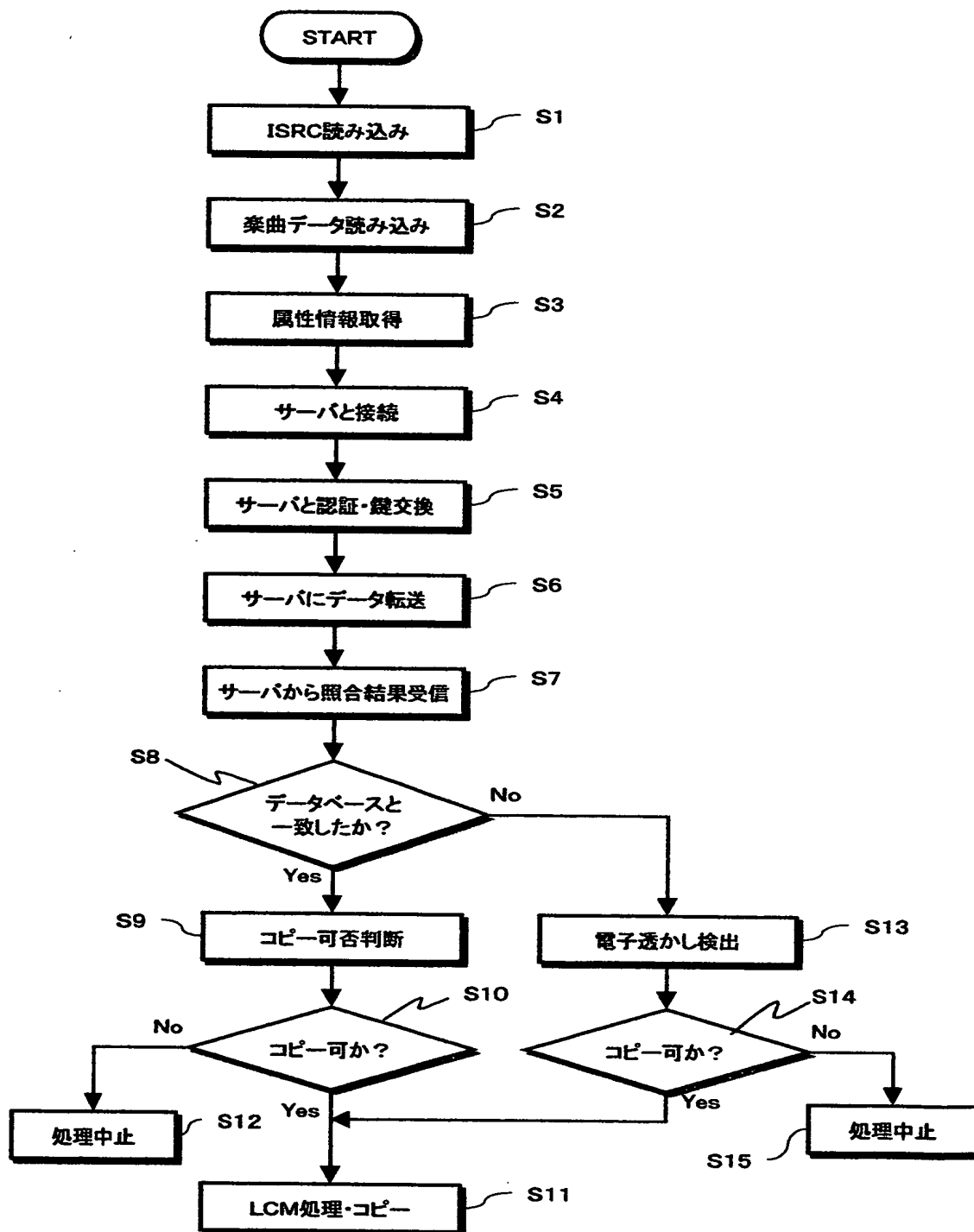
【図 1】



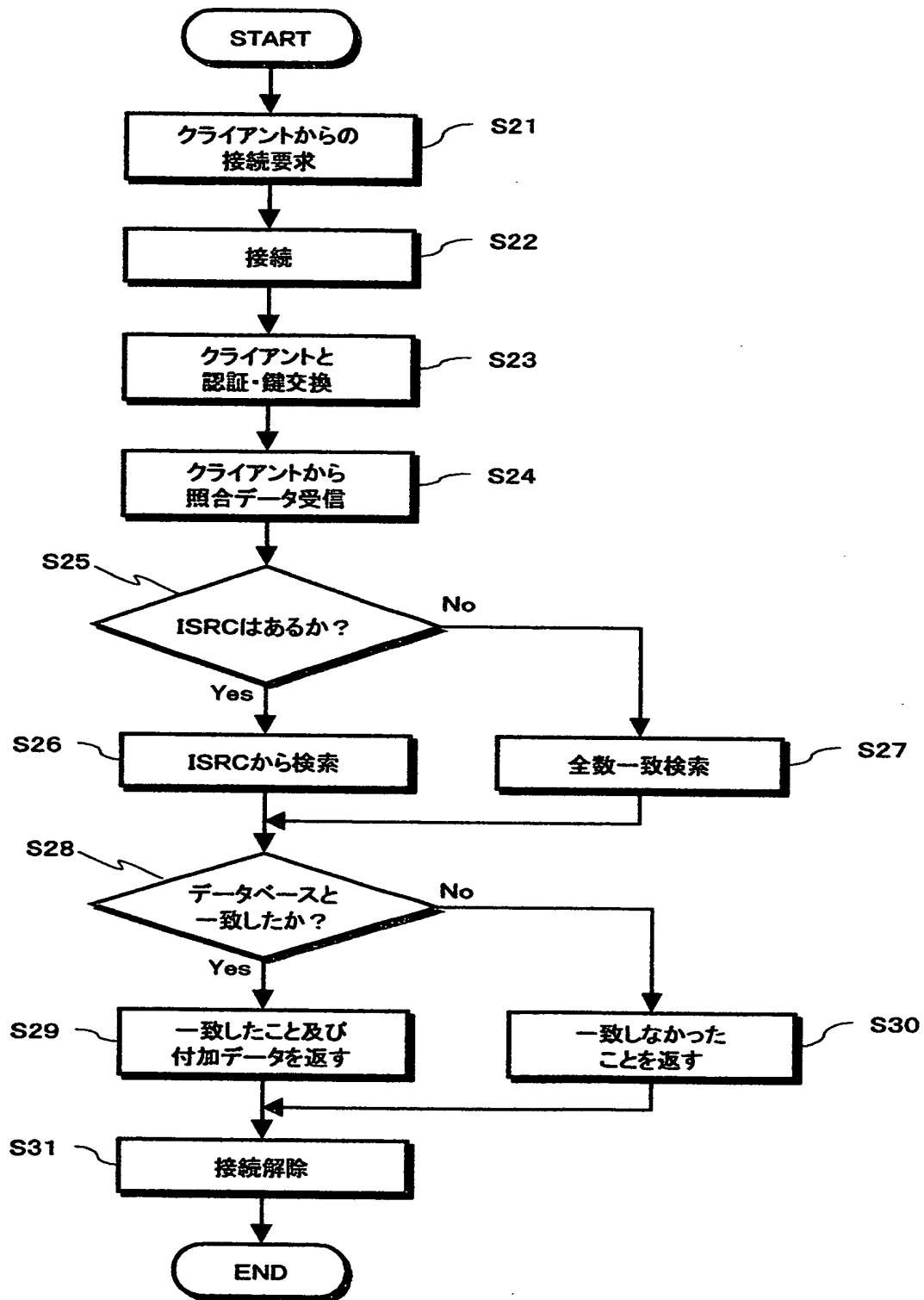
【図2】



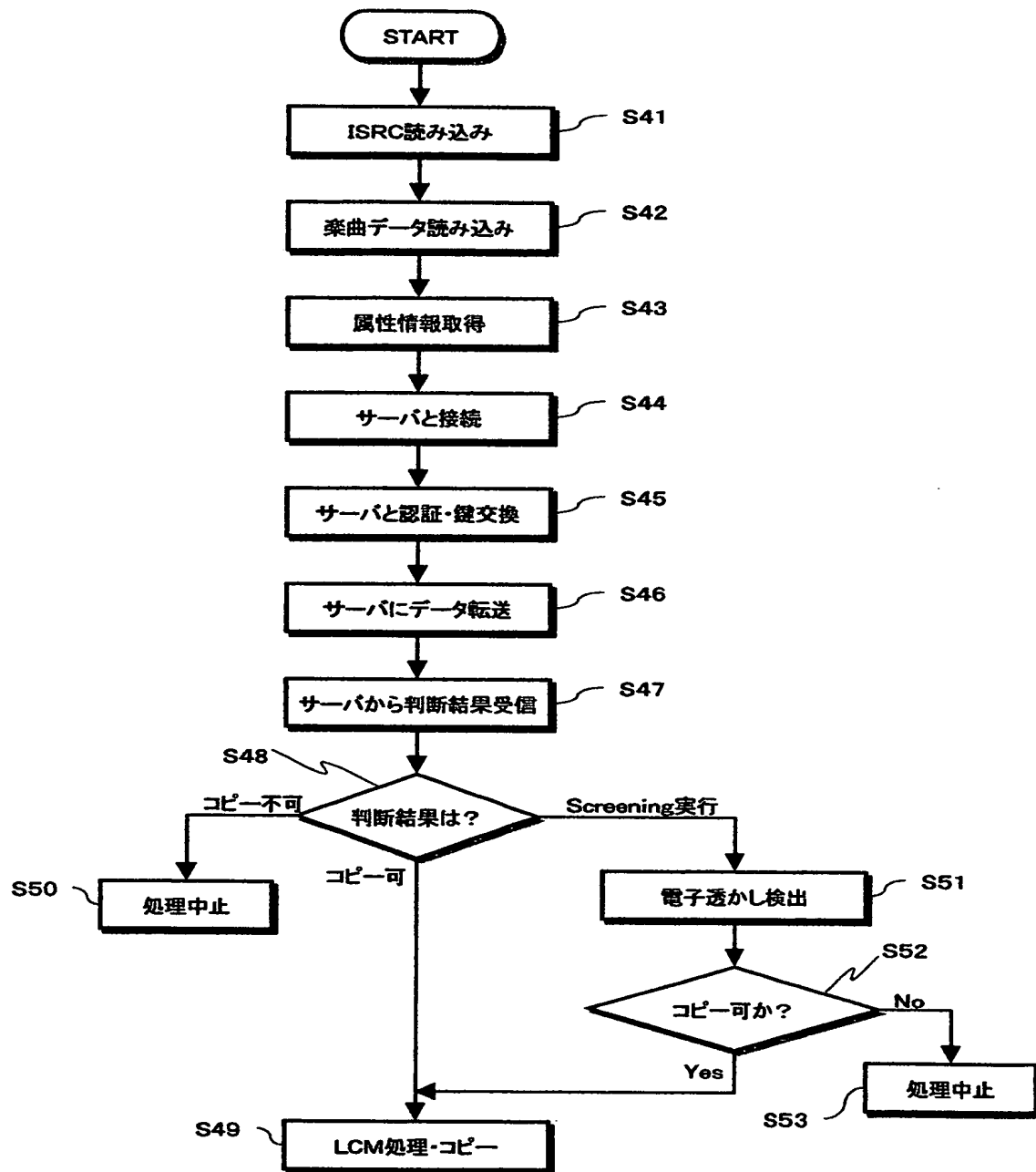
【図 3】



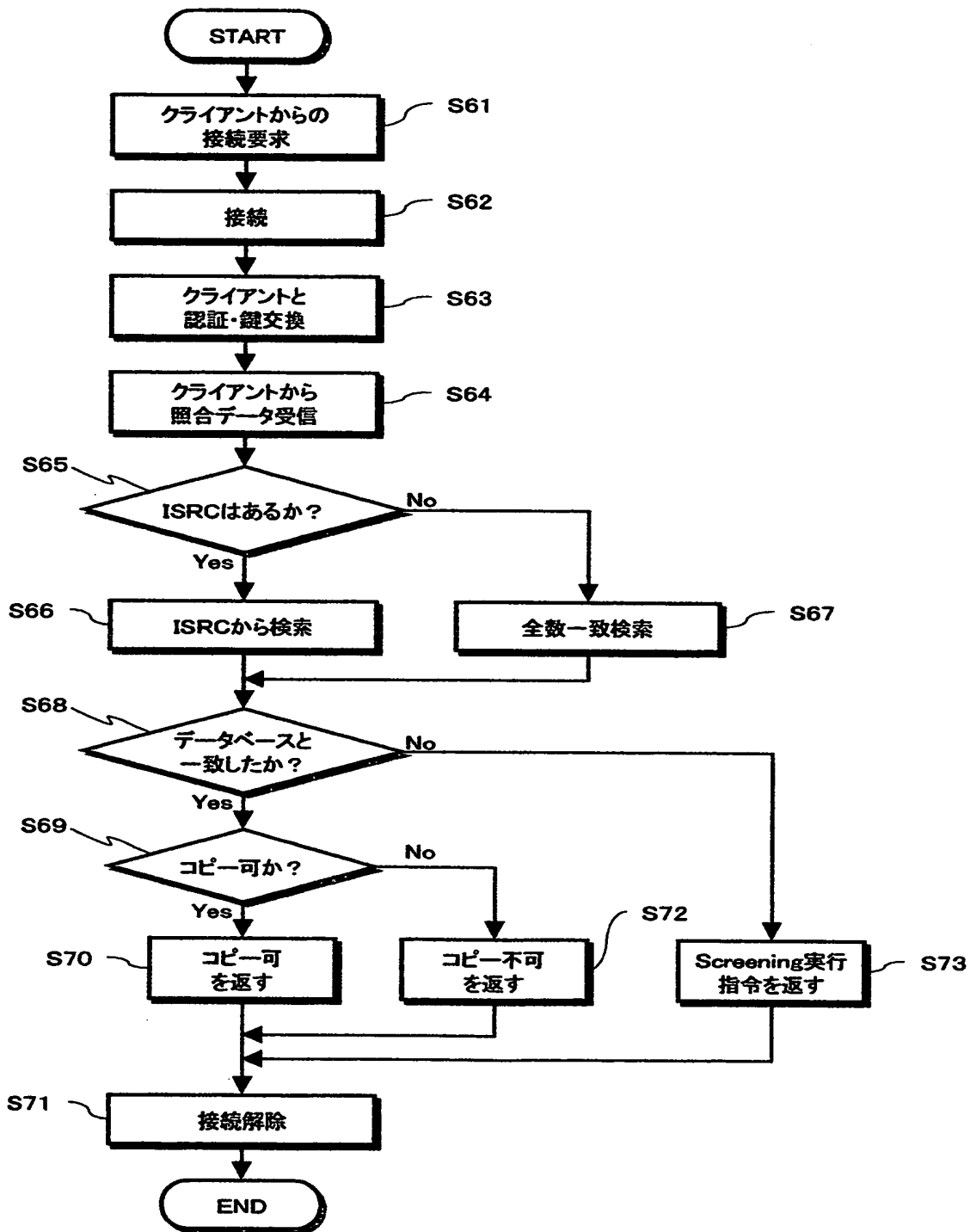
【図 4】



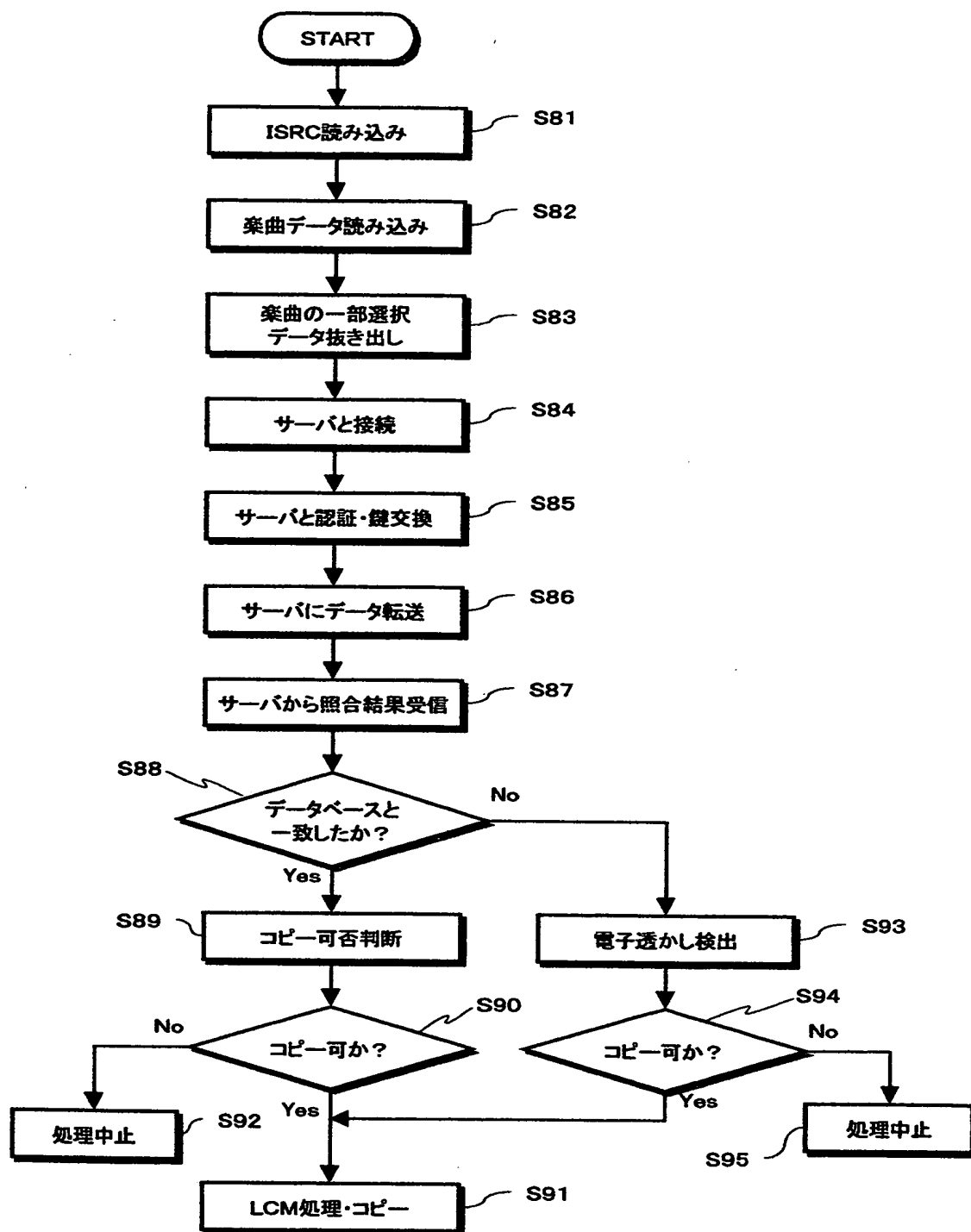
【図5】



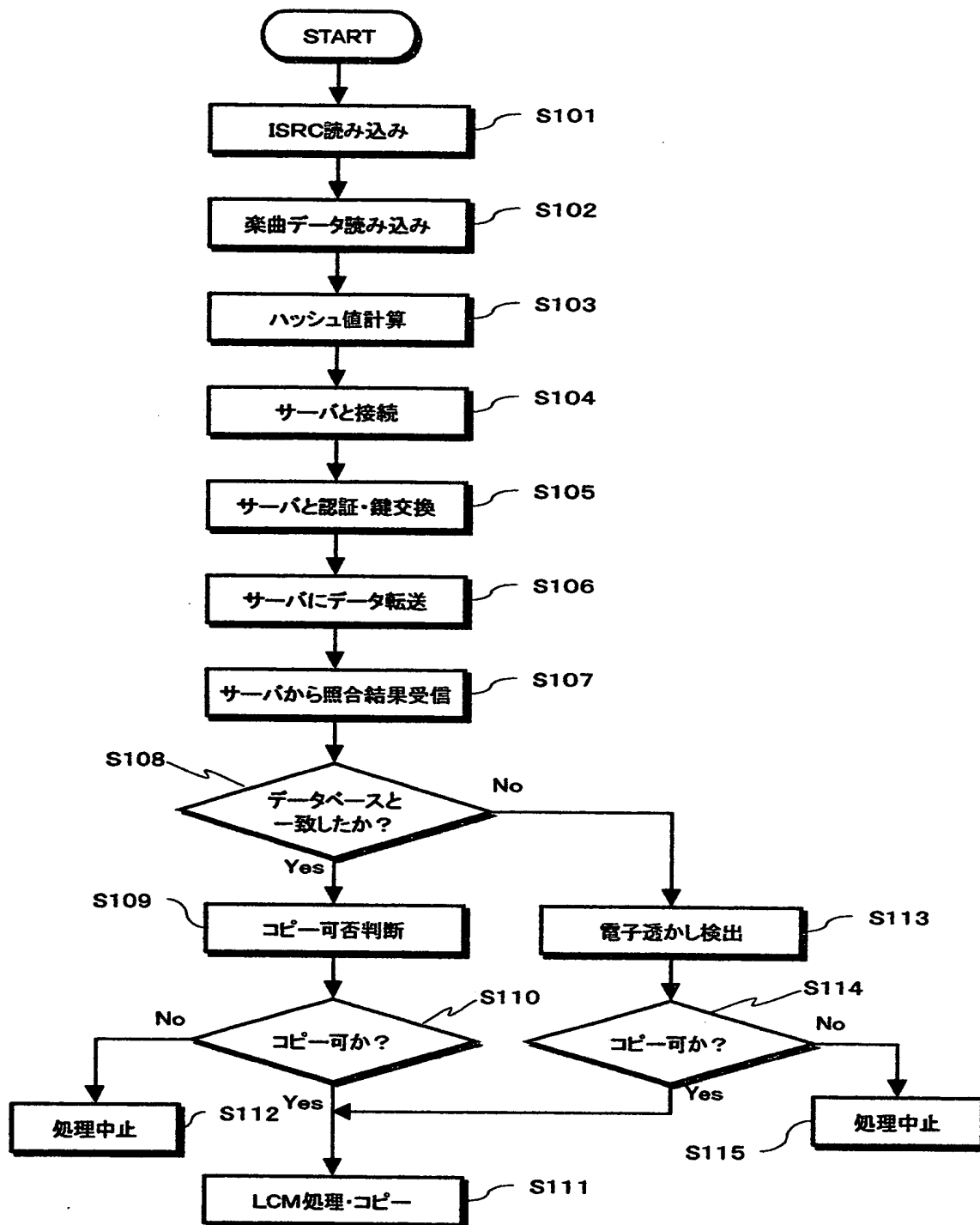
【図6】



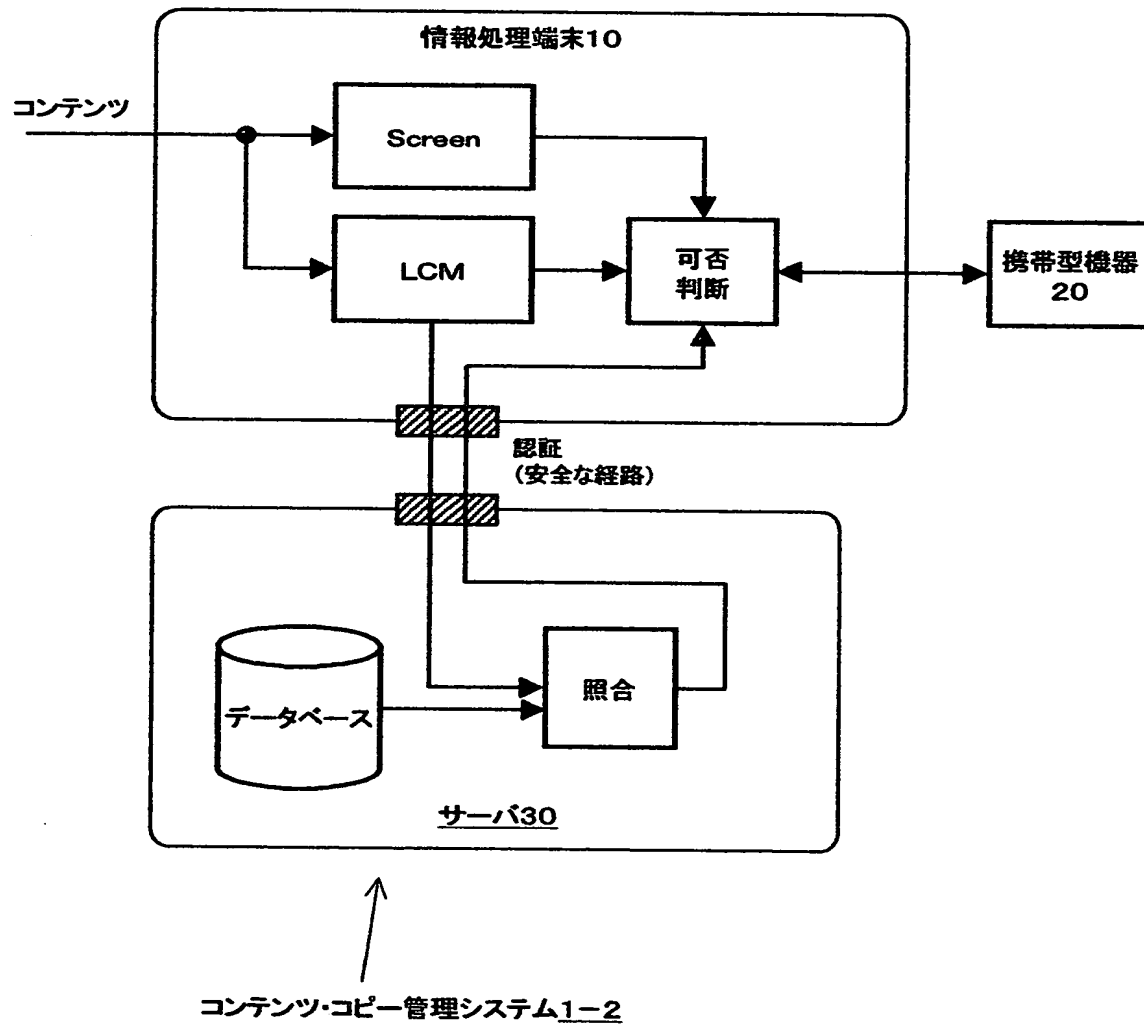
【図 7】



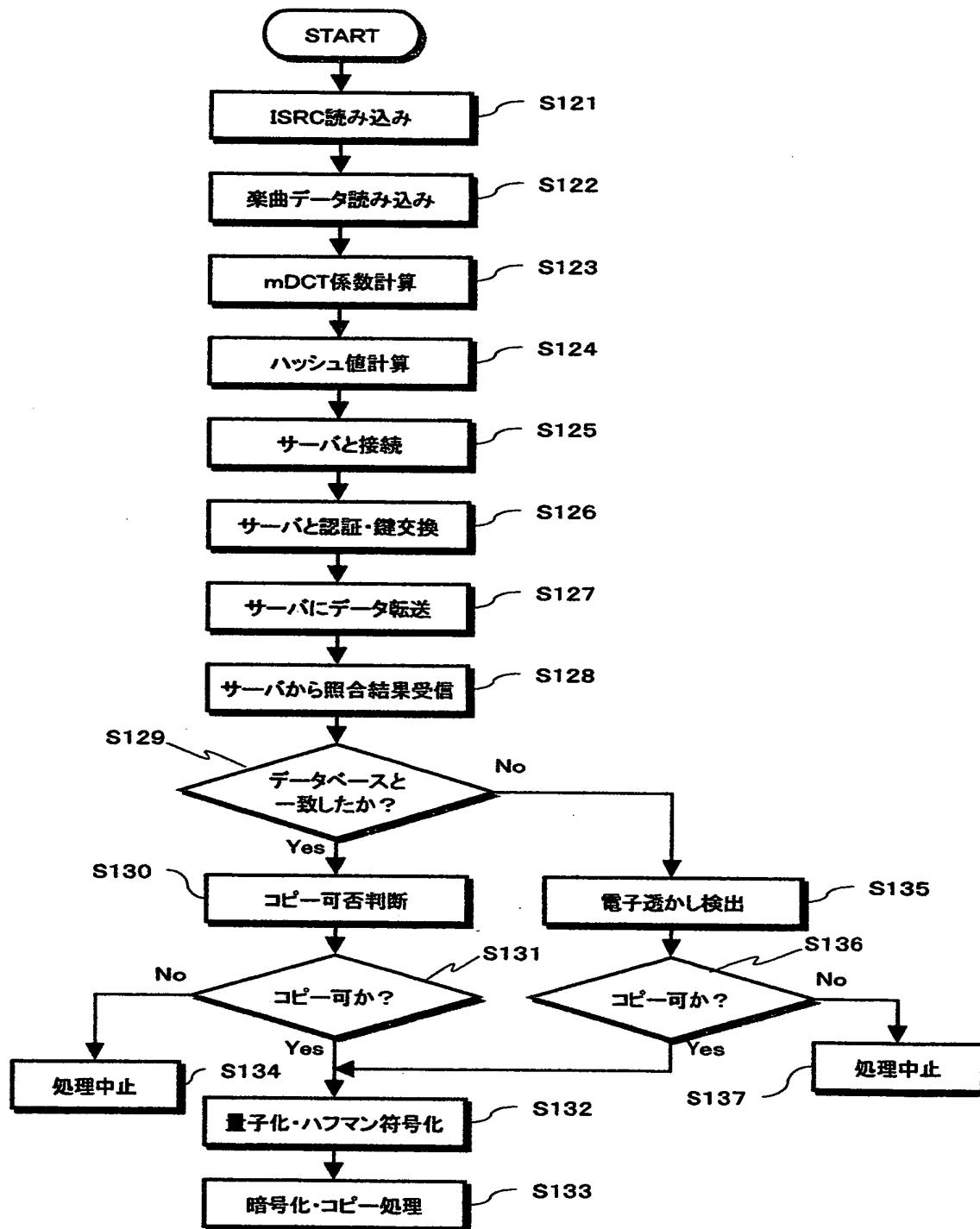
【図 8】



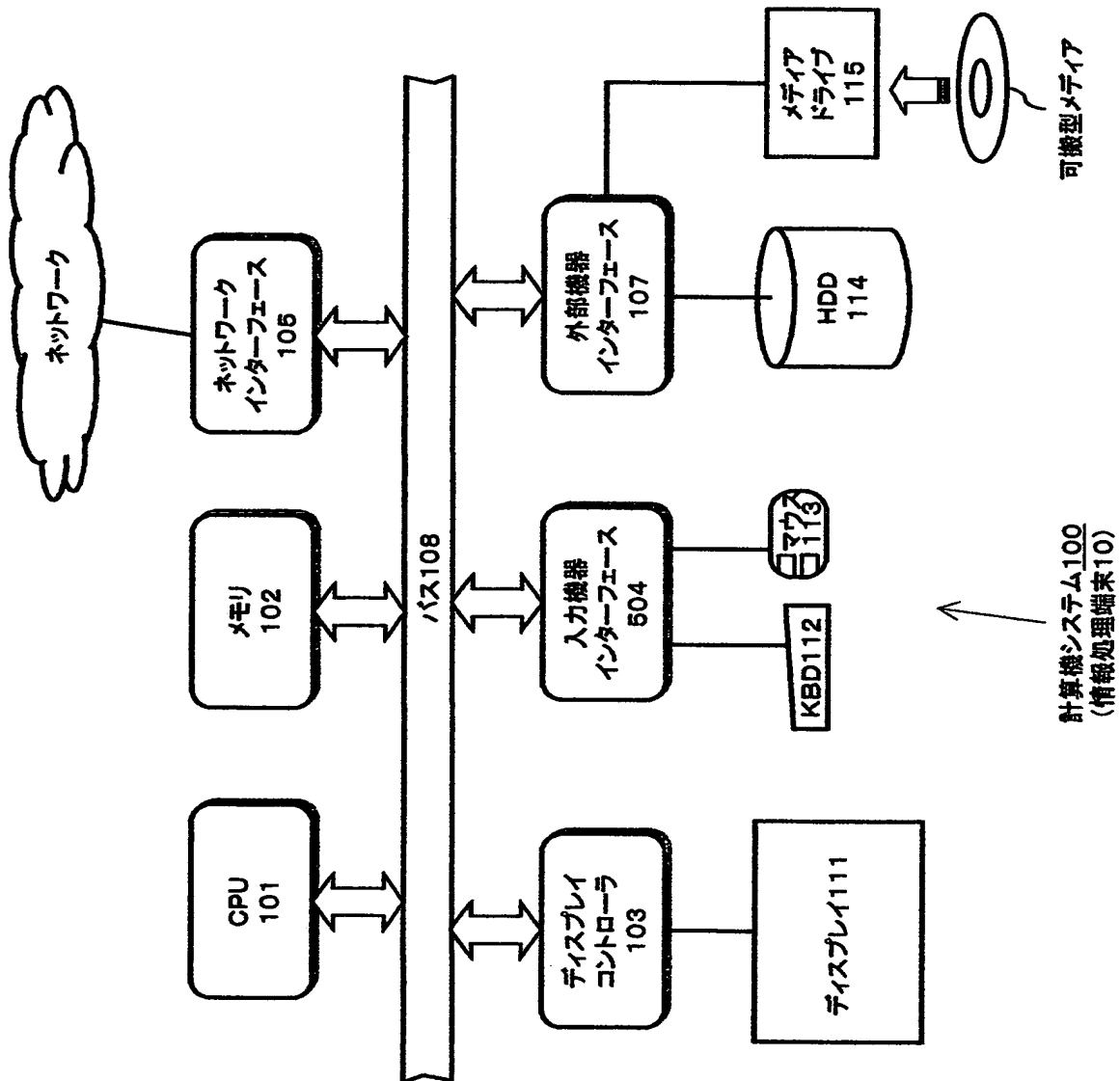
【図 9】



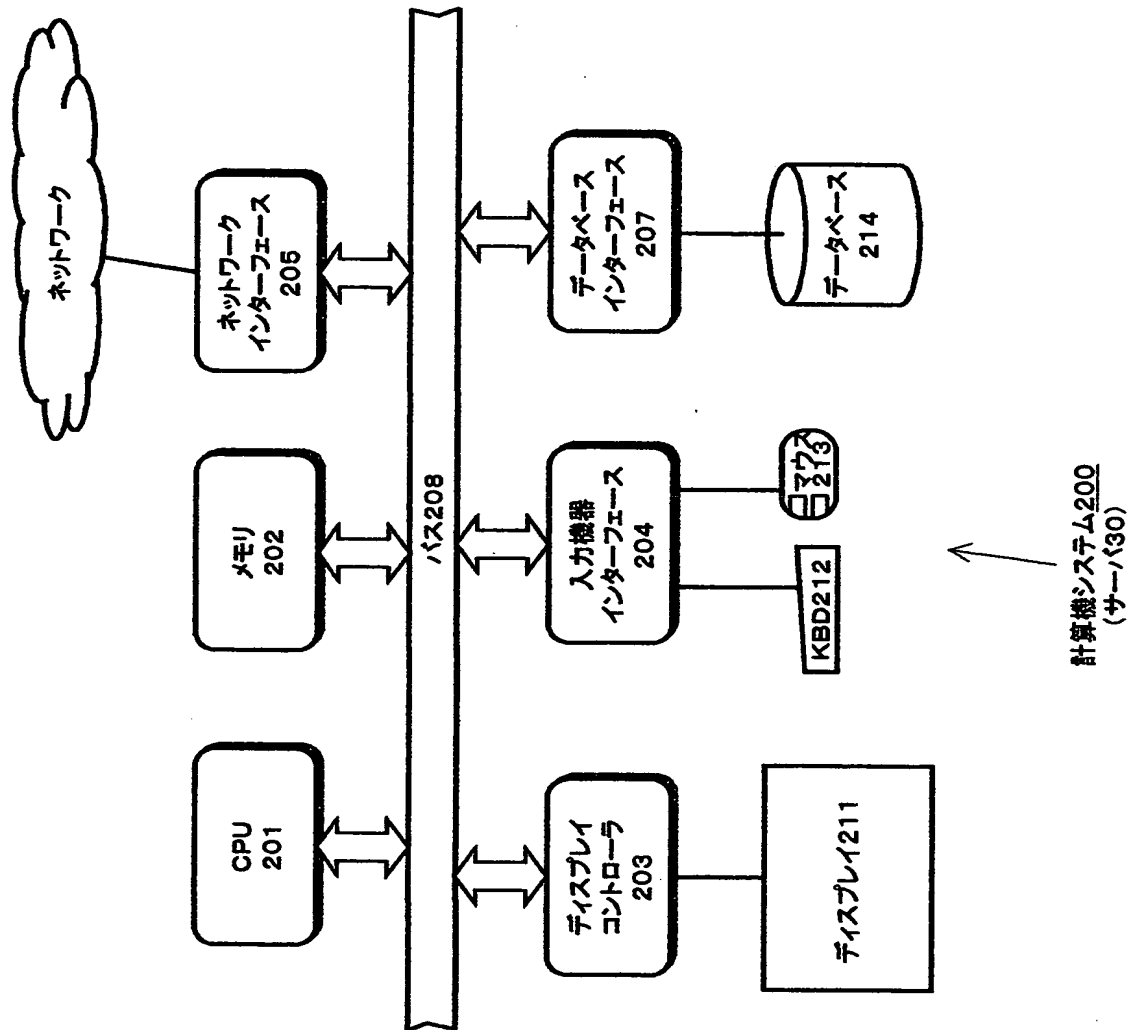
【図10】



【図 11】



【図 12】



【書類名】 要約書

【要約】

【課題】 計算負荷の高い電子透かし検査処理を代行して、コンテンツの複製の可否を判断する。

【解決手段】 コンテンツの複製を行う計算機システム自体がスクリーニングすなわち電子透かしの検出を必ずしも行わず、外部サーバのような別の手段により、コンテンツのコピー制御情報を取得できるようにした。例えば、コンテンツには電子透かしが挿入されていないことがあらかじめ分かっているCDからコピーするような場合には、かかるCDであることを確認できれば、電子透かしの検出処理そのものをスキップして、コピー所要時間を短縮化する。

【選択図】 図2

認定・付加情報

特許出願の番号	特願 2001-103153
受付番号	50100482374
書類名	特許願
担当官	第三担当上席 0092
作成日	平成 13 年 4 月 5 日

<認定情報・付加情報>

【特許出願人】

【識別番号】	000002185
【住所又は居所】	東京都品川区北品川 6 丁目 7 番 35 号
【氏名又は名称】	ソニー株式会社

【代理人】

申請人

【識別番号】	100101801
【住所又は居所】	東京都中央区新富 1-1-7 銀座ティーケイビル 6 階 澤田・宮田・山田特許事務所
【氏名又は名称】	山田 英治

【選任した代理人】

【識別番号】	100093241
【住所又は居所】	東京都中央区新富 1-1-7 銀座ティーケイビル 6 階 澤田・宮田・山田特許事務所
【氏名又は名称】	宮田 正昭

【選任した代理人】

【識別番号】	100086531
【住所又は居所】	東京都中央区新富 1-1-7 銀座ティーケイビル 6 階 澤田・宮田・山田特許事務所
【氏名又は名称】	澤田 俊夫

出 願 人 履 歴 情 報

識別番号 [000002185]

1. 変更年月日 1990年 8月30日

[変更理由] 新規登録

住 所 東京都品川区北品川6丁目7番35号

氏 名 ソニー株式会社